hp StorageWorks

edge switch 2/32 installation guide

Part Number: AA-RSTZB-TE/958-000290-000

Second Edition (January 2003)

This installation guide provides procedures for setting up, configuring, and managing the Edge Switch 2/32.

hp

i n v e n t

Contents

About This Guide

2   Installing and Configuring the Edge Switch 2/32

B Technical Specifications

Glossary

Index

Figures

Tables

About This Guide

This installation guide provides information to help you:

- Set up the Edge Switch 2/32.

- Configure the Edge Switch 2/32.

- Manage the Edge Switch 2/32.

- Contact technical support for additional assistance.

Intended Audience

This book is intended for use by administrators who are experienced with the following:

- Fibre Channel technology

- StorageWorks Fibre Channel Switches by HP

Related Documentation

For a list of corresponding documentation included with this product, see the "Related Documents" section of the *hp StorageWorks edge switch release notes*.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks website:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Industry Association website, located at http://www.fibrechannel.org.

Document Conventions

The conventions included in Table 1 apply.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command names, system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase unless they are case sensitive
Variables	*`Monospace, italic font`*
Website addresses	Sans serif font (http://thenew.hp.com)

Symbols in Text

These symbols may be found in the text of this manual. They have the following meanings.

> **WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.**

> **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

> **Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.**
>
> **WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.**

> **Any RJ-45 receptacle marked with these symbols indicates a network interface connection.**
>
> **WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.**

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.
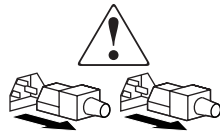
Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- **The leveling jacks are extended to the floor.**
- **The full weight of the rack rests on the leveling jacks.**
- **In single rack installations, the stabilizing feet are attached to the rack.**
- **In multiple rack installations, the racks are coupled.**
- **Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.**

Getting Help

If you still have a question after reading this manual, contact an HP authorized service provider or access our website: http://thenew.hp.com.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

NOTE: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://thenew.hp.com/country/us/eng/support.html.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)

- Product serial numbers

- Product model names and numbers

- Applicable error messages

- Operating system type and revision level

- Detailed, specific questions

HP Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://thenew.hp.com/country/us/eng/prodserv/storage.html. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP Authorized Reseller:

- In the United States, call 1-800-345-1518

- In Canada, call 1-800-263-5868

- Elsewhere, see the HP website for locations and telephone numbers: http://thenew.hp.com.

1

Introduction

The HP StorageWorks Edge Switch 2/32 provides dynamic switched connections between Fibre Channel servers and devices in a storage area network (SAN) environment. SANs introduce the concept of server-to-device networking and multi-switch fabrics, eliminate requirements for dedicated connections, and enable the enterprise to become data centric.

A SAN provides speed, high capacity, and flexibility for the enterprise, and is primarily based upon Fibre Channel architecture. The switch implements Fibre Channel technology that provides a bandwidth of 2.125 Gbps, redundant switched data paths, a scalable number of active ports, and long transmission distances (up to 35 km).

This chapter describes the switch and attached HP StorageWorks Ha-Fabric Manager (HAFM) server. The chapter specifically discusses:

- Switch management, error-detection and reporting features, serviceability features, zoning, multi-switch fabrics, and specifications.

- The HAFM server and minimum hardware specifications.

- Remote workstation configurations and hardware specifications.

- Maintenance approach.

- Field-replaceable units (FRUs).

- Connectors and indicators.

- Software diagnostic features.

- Tools and test equipment.

Edge Switch 2/32 Description

The switch can be installed on a table or desk top, or mounted in an equipment cabinet or in any standard equipment rack.

Multiple switches and the HAFM server communicate on a local area network (LAN) through one or more 10Base-T Ethernet hubs. One or more 24-port Ethernet hubs are optional and can be ordered with the switch. Up to three hubs are daisy-chained as required to provide additional Ethernet connections as more switches (or other HP managed products) are installed on a customer network.

Figure 1–1 illustrates the switch, HAFM server, and Ethernet hub.
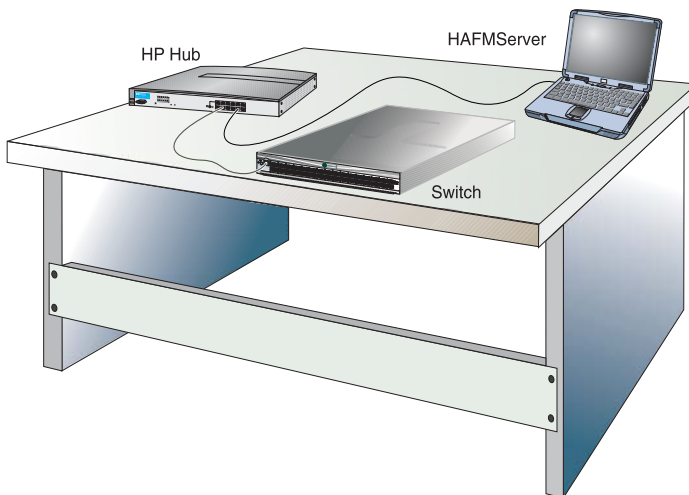
Figure 1–1: Switch, HAFM server, and Ethernet hub

The switch provides dynamic switched connections for servers and devices, supports mainframe and open-systems interconnection (OSI) computing environments, and provides data transmission and flow control between device node ports (N_Ports) as dictated by the Fibre Channel Physical and Signaling Interface (FC-PH 4.3). Through interswitch links (ISLs), the switch can connect additional switches to form a Fibre Channel multi-switch fabric.

The switch provides connectivity for devices manufactured by multiple original equipment manufacturers (OEMs). To determine if an OEM product can communicate through connections provided by the switch, or if communication restrictions apply, refer to the supporting publications for the product or contact your HP marketing representative.

Features

The following sections describe the features of the Edge Switch 2/32:

Error-Detection, Reporting, and Serviceability

The switch provides the following error-detection, reporting, and serviceability features:

- Light-emitting diodes (LEDs) on switch FRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.

- System and threshold alerts, event logs, audit logs, link incident logs, threshold alert logs, and hardware logs that display switch, Ethernet link, and Fibre Channel link status at the HAFM server.

- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (internal loopback, external loopback, and Fibre Channel (FC) loopback tests). The FC loopback test applies only when the switch is configured to operate in S/390 mode.

- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature at the HAFM server.

- A modem for use by support personnel to dial-in to the HAFM server for event notification and to perform remote diagnostics.

- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's internet protocol (IP) address, subnet mask, and gateway address. Or to run diagnostics and isolate system problems through a local or remote terminal.

- Redundant FRUs—small form factor pluggable (SFP) optical transceivers, power supplies, and cooling fans—that are removed or replaced without disrupting switch or Fibre Channel link operation.

- A modular design that enables quick removal and replacement of FRUs without tools or equipment.

- Concurrent port maintenance—SFPs and fiber-optic cables are removed and attached to ports without interrupting other ports or director operation.

- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.

- Data collection through the *Product Manager* application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.

- Simple network management protocol (SNMP) management using the Fibre Alliance MIB that runs on the HAFM server. Up to 12 authorized management workstations can be configured through the *HAFM* application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

- SNMP management using the Fibre Channel Fabric Element MIB (Version 1.10), transmission control protocol/internet protocol (TCP/IP) MIB-II definition (RFC 1213), or a product-specific MIB that run on each switch. Up to 12 authorized management workstations can be configured through the *Product Manager* application to receive unsolicited SNMP trap messages. The trap messages indicate switch operational state changes and failure conditions.

NOTE: For more information about SNMP support provided by HP products, refer to the hp StorageWorks SNMP reference guide for director 2/64, edge switch 2/16, and edge switch 2/32.

Zoning

The switch supports a name server zoning feature that partitions attached devices into restricted-access groups called zones. Devices in the same zone can recognize and communicate with each other through switched port-to-port connections. Devices in separate zones cannot communicate with each other.

Zoning is configured by authorizing or restricting access to name server information associated with device N_Ports that attach to switch fabric ports (F_Ports). A zone member is specified by the port number to which a device is attached, or by the eight-byte (16-digit) World Wide Name (WWN) assigned to the host bus adapter (HBA) or Fibre Channel interface installed in a device. A device can belong to multiple zones.

$\triangle$ **CAUTION:** If zoning is implemented by port number, a change to the switch fiber-optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

If zoning is implemented by WWN, removal and replacement of a device HBA or Fibre Channel interface (thereby changing the device WWN) disrupts zone operation and may incorrectly include or exclude a device from a zone.

In Open Fabric mode, only zoning by WWN is supported. Zoning by port numbers is not.

Zones are grouped into zone sets. A zone set is a group of zones that is enabled (activated) or disabled across all switches in a multi-switch fabric. Only one zone set can be enabled at one time.

Multi-Switch Fabrics

A Fibre Channel topology that consists of one or more interconnected switches or switch elements is called a fabric. Operational software provides the ability to interconnect switches (through expansion port (E_Port) connections) to form a multi-switch fabric. The data transmission path through the fabric is typically determined by fabric elements and is user-transparent. Subject to zoning restrictions, devices attached to any interconnected switch can communicate with each other through the fabric.

Switch Management

These options are available for managing the Edge Switch 2/32 through a user interface:

- The *Product Manager* application installed on an High Availability Fabric Manager (HAFM) server. Access to the Product Manager must be through the *HAFM* applications. These applications are installed on the HAFM server.

- The Embedded Web Server interface. Using a browser-capable PC with an internet connection to the switch, you can monitor and manage the switch through the web server interface embedded in the switch firmware. The interface provides a GUI similar to the *Product Manager* application and supports switch configuration, statistics monitoring, and basic operation.

  To launch the Embedded Web Server interface, enter the switches IP address as the internet uniform resource locator (URL) into any standard browser. Enter a user name and password at a the login screen. The browser then becomes a management console. Refer to the web server interface online help for details on use.

  NOTE: The default user name for the right to view status and other information is `operator`. The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is `administrator`. The default password for both user names is `password`.

- The command line interface (CLI). The CLI allows you to access many HAFM and Product Manager functions while entering commands during a Telnet session with the switch. The primary purpose of the CLI is to automate management of a large number of switches using scripts. The CLI is not an interactive interface; no

checking is done for pre-existing conditions and no prompts display to guide users through tasks. Refer to *hp StorageWorks CLI reference guide for edge switches and directors*.

This manual provides details on the *Product Manager* application for the Edge Switch 2/32 only. Use this manual for the Product Manager installed on an HAFM server. This manual does not cover the Embedded Web Server interface or CLI.

Field Replaceable Units

The switch provides a modular design that enables quick removal and replacement of FRUs small form factor pluggable SFP optical transceivers, power supplies, and fans. Figure 1–2 illustrates the front of the switch. The switch front panel includes:
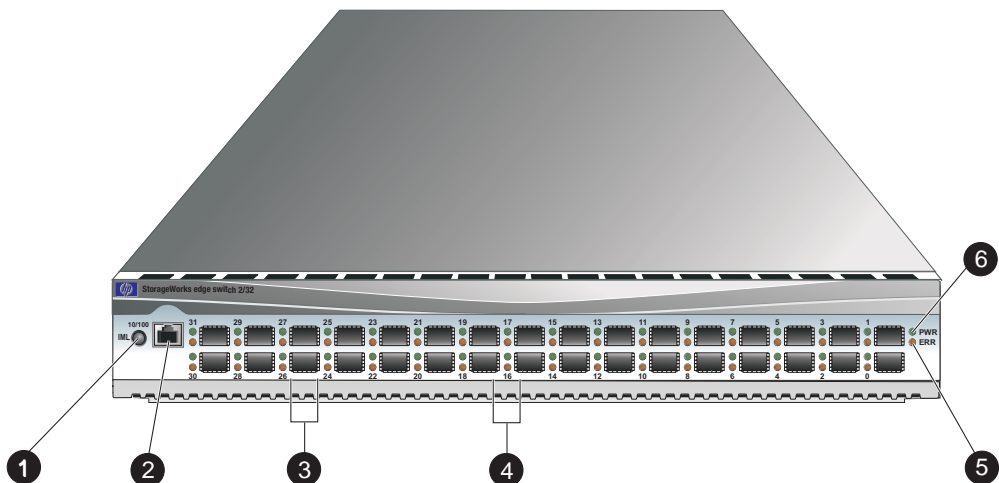
SHR-2369

❶ Initial machine load (IML) button ❹ Port LEDs
❷ Ethernet LAN connector ❺ Error LED (amber)
❸ SFP fiber optic connectors ❻ Power LED (green)

Figure 1–2: Edge Switch 2/32 (Front View)

Figure 1–3 illustrates the rear of the switch. The FRUs on the rear panel include two power supplies and four individual cooling fan FRUs. Also shown on the rear panel is an RS-232 maintenance port (not labeled).

❶	Cooling fan (4)	❸	Power switches on power supplies (2)
❷	Power supply (2)		
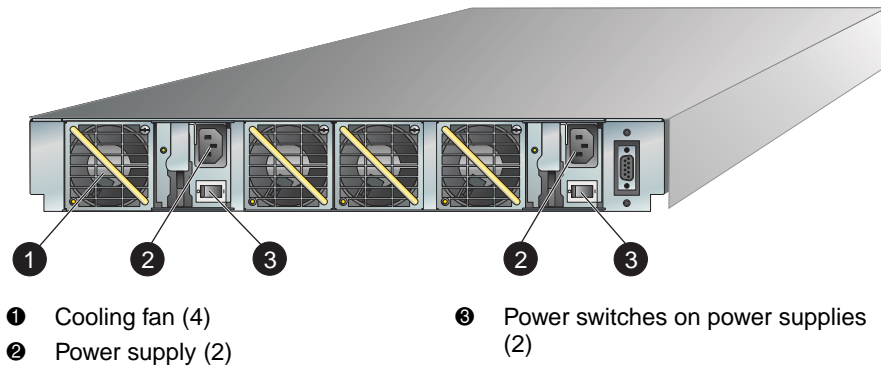
Figure 1–3: Edge Switch 2/32 (Rear View)

SFP Transceivers

A single-mode or multi-mode fiber-optic cable attaches to a port through a pluggable small form factor (SFP) transceiver. The SFP provides a duplex LC interface, and can be detached from the switch port for easy replacement. Two fiber-optic transceiver types are available:

- **Shortwave laser —** Shortwave laser SFPs provide short-distance connections (2 to 500 meters) through 50-micron or 62.5-micron multi-mode fiber.

- **Longwave laser —** Longwave laser SFPs provide long-distance connections (up to 10 kilometers) through 9-micron single-mode fiber.

Cooling Fans

Four fans (each a separate FRU) provide cooling for the switch power supplies and the control processor (CTP) card, as well as redundancy for continued operation if a single fan fails.

Each fan FRU can be replaced while the switch is operating.

Power Supplies

Redundant, load-sharing power supplies step down and rectify facility input power to provide 3.3 volts direct current (VDC), 5 VDC, and 12 VDC to the CTP. The power supplies also provide input filtering, overvoltage protection, and overcurrent protection. Either power supply can be replaced while the switch is operational.

Each power supply has a separate CTP connection to allow for independent AC power sources. The power supplies are input-rated at 100 to 230 volts alternating current (VAC).

Power supply requirements are listed in Appendix B.

Connectors and Indicators

Connectors and indicators include the:

- Initial machine load (IML) button.

- Ethernet LAN connector.

- Green power (PWR) and amber system error (ERR) LEDs.

- Green and amber status LEDs associated with FRUs.

- RS-232 maintenance port.

Initial Machine Load Button

When the IML button, as shown in Figure 1–2 is pressed and held for three seconds, the switch performs an IML that takes approximately 30 seconds and resets the:

- Microprocessor and functional logic for the CTP and loads firmware from FLASH memory.

- Ethernet LAN interface, causing the connection to the HAFM server to drop momentarily until the connection automatically recovers.

- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover.

An IML should only be performed if a CTP failure is indicated. Do not IML the switch unless directed to do so by a procedural step or the next level of support. As a precaution, the IML button is flush mounted to protect against accidental activation.

Ethernet LAN Connector

The front panel provides a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector, as shown in Figure 1–2 that attaches to an Ethernet LAN to provide communication with the HAFM server or an SNMP management workstation. Two green LEDs are associated with the LAN connector. When illuminated, the left LED indicates LAN operation at 10 Mbps, and the right LED indicates LAN operation at 100 Mbps.

Power and System Error LEDs

The PWR LED, as shown in Figure 1–2 illuminates when the switch is connected to facility AC power and powered on. If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The ERR LED, as shown in Figure 1–2 illuminates when the switch detects an event requiring immediate operator attention, such as a FRU failure. The LED remains illuminated as long as an event is active. The LED extinguishes when the Clear System Error Light function is selected from the *Product Manager* application. The LED blinks if unit beaconing is enabled. An illuminated ERR LED (indicating a failure) takes precedence over unit beaconing.

FRU Status LEDs

Amber and green LEDs associated with switch FRUs provide status information as follows:

- **Port SFP —** Amber and green LEDs to the left of the port, as shown in Figure 1–2 illuminate, extinguish, or blink to indicate various port states (operational with active Fibre Channel traffic, operational but not communicating, beaconing, blocked, failed, inactive, or running diagnostics).

- **Fan —** An amber LED at the lower left corner of each fan, as shown in Figure 1–3 illuminates if the fan fails or rotates too slowly.

- **Power Supply —** A green LED at the upper left corner of each power supply, as shown in Figure 1–3 illuminates if the power supply is operational and receiving AC power.

Maintenance Port

The rear panel provides a 9-pin RS-232 maintenance port, as shown in Figure 1–3 that provides a connection for a local terminal or dial-in connection for a remote terminal. Although the port is typically used by authorized maintenance personnel, operations personnel can use the port to configure switch network addresses.

Software Diagnostic Features

The switch provides the following diagnostic software features that aid in fault isolation and repair of problems:

- FRUs provide on-board diagnostic and monitoring circuits that continuously report FRU status to the *HAFM* and *Product Manager* applications. These applications provide system alerts and logs that display failure and diagnostic information at the HAFM server or a remote workstation communicating with the HAFM server.

- The HAFM Services application that runs as a Windows 2000 service and provides an additional user interface to display operational status.

- The Embedded Web Server interface that provides Internet access to isolate problems for a single switch.

- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to 12 authorized management workstations.

- E-mail messages or call-home reports provide automatic notification of significant system events to designated support personnel or administrators.

HAFM Server Description

The HAFM server, as shown in Figure 1–4 is a notebook personal computer (PC) that provides a central point of control for up to 48 LAN-connected directors or Edge Switches.

Figure 1–4: HAFM server

The server is mounted in a slide-out drawer in the HP-supplied equipment rack. The HAFM server or Ethernet access to the Embedded Web Server (EWS) interface is required to install, configure, and manage the Edge Switch 2/32.

Although a configured switch operates normally without HAFM server intervention, an attached server should operate at all times to monitor switch operation, log events and configuration changes, and report failures.

The HAFM server provides an auto-detecting 10/100 Mbps LAN connection, provided by an internal Ethernet adapter card. This LAN port attaches to the customer's public intranet to allow access from remote user workstations. An optional Ethernet adapter card (not supplied by HP) can be installed in the personal computer memory card international association (PCMCIA) slot to provide a connection to a private LAN segment for dedicated director communication.

Ethernet Hub

The HAFM server and managed directors connect through a rack-mounted 10/100 Base-T Ethernet hub. Figure 1–5 illustrates the optional 12-port hub.
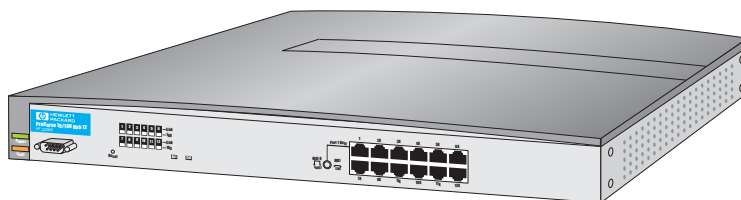
Figure 1–5: 12-Port Ethernet hub

Optional Kits

Contact your HP authorized service provider to purchase the following optional edge switch 2/32 kits. See Table 1–1.

Table 1–1: Edge switch 2/32 Optional Kits

Supporting Kit	Description
8-flexport upgrade for Edge Switch 2/32, Part Number: DS-DM8PU-AA / 302660-B21	Used to upgrade from 16 to 24 and 24 to 32 ports.
2/32 Product Manager license, Part Number: QM-6YCAA-AA / 300658-B21	Used when switch is managed through HAFM.

2

Installing and Configuring the Edge Switch 2/32

This chapter describes tasks to install, configure, and verify operation of the edge switch 2/32. The switch can be installed on a table or desk top, or mounted in any standard equipment rack.

For a list of the factory-set defaults for the switch and the Reset Configuration option, refer to Appendix B.

Summary of Installation Tasks

Table 2–1 summarizes installation tasks for the switch, HAFM server, and Ethernet hub. The table numbers and describes each task, states if the task is required or optional, and lists the page reference for the task. If a task is optional, decision-related information is included.

Table 2–1: Installation Task Summary

Task Number and Description	Required or Optional	Page
Task 1: Verify Installation Requirements	Required	2–3
Task 2: Unpack, Inspect, and Install the Switch	Required	2–4
Task 3: Configure Network Information	Optional—configure if connecting multiple switches or if connecting a switch and HAFM server to a public LAN.	2–6
Task 4: LAN-Connect the Switch	Required	2–11
Task 5: HAFM Server (Optional)	Optional—if not done, then the switch should be configured using the Embedded Web Server (EWS) interface.	2–12

Table 2–1: Installation Task Summary (Continued)

Task Number and Description	Required or Optional	Page
Task 6: Configure the Switch to the HAFM Application	Required if Task 5: HAFM Server (Optional) task was done.	2–13
Task 7: Record or Verify HAFM Server Restore Information	Required if Task 5: HAFM Server (Optional) task was done.	2–13
Task 8: Verify Switch-to-HAFM Server Communication	Required if Task 5: HAFM Server (Optional) task was done.	2–14
Task 9: Configure Feature Key (Optional)	Optional—configure if a feature key is ordered by the customer.	2–15
Task 10: Configure OSMS or FICON Management Server (Optional)	Optional—configure if the HAFM server is installed.	2–19
Task 11: Set Switch Date and Time	Optional	2–21
Task 12: Configure the Edge Switch 2/32 Product Manager Applications	Required	2–23
Task 13: Test Remote Notification (Optional)	Optional	2–50
Task 14: Back Up HAFM Configuration Data	Required	2–51
Task 15: Configure the Switch from the Embedded Web Server (Optional)	Optional—if not done, then the switch should be configured using the HAFM server.	2–51
Task 16: Cable Fibre Channel Ports	Required	2–69
Task 17: Connect Switch to a Fabric (Optional)	Optional—perform this task to connect the switch to a fabric.	2–69
Task 18: Unpack, Inspect, and Install the Ethernet Hub (Optional)	Optional—install only if ordered and Ethernet segment does not exist to connect switches and the HAFM server.	2–71

Installation Options

The switch is installed in one of two configurations. The options are:

- **Table or desk top**—one or more switches, an optional HAFM server, and an optional Ethernet hub are delivered and installed at the customer facility on a desk or table top. Ethernet cabling distance, and local area network (LAN) addressing issues must be considered.

- **Customer-supplied equipment rack**—one or more switches, an optional HAFM server, and an optional Ethernet hub are delivered to the customer facility for installation in a customer-supplied equipment rack. Rack-mount hardware is provided in the shipping container. Ethernet cabling, distance, and LAN addressing issues must be considered.

Task 1: Verify Installation Requirements

Verify the following requirements are met prior to switch and HAFM server installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Fabric and device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *hp StorageWorks product in a SAN environment: planning guide for director 2/64, edge switch 2/16, and edge switch 2/32*.

- Support equipment and personnel are available for the installation.

- The required number and type of fiber-optic jumper cables are delivered and available. Ensure the cables are the correct length with the required connectors.

- A customer-supplied equipment rack and associated hardware are available (optional).

- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a corporate or dedicated LAN.

Task 2: Unpack, Inspect, and Install the Switch

The following paragraphs provide instructions to unpack and inspect the edge switch 2/32, and install it in a desktop or rack-mount configuration.

Unpack and Inspect the Switch

Unpack and inspect the switch:

<table>
<tr><td>⚠</td><td>CAUTION: When you remove the switch from the carton, do not rest it on its rear window while examining it. To do so may break the FRU handles.</td></tr>
</table>

1. Inspect the shipping containers for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.

2. Unpack the shipping containers and inspect each item for damage. Save all shipping and packing materials. Ensure that all items on the enclosed shipping list are in each container.

3. If any items are damaged or missing, customers should contact a HP authorized service provider or reseller.

Desktop Installation

To install and configure the switch on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of the switch. Ensure the pads are aligned with the scribed circles at each corner.

2. Position the switch on a table or desktop as directed by the customer. Ensure:

   • Grounded AC electrical outlets are available.

   • Adequate ventilation is present.

   • Areas with excessive heat, dust, or moisture are avoided.

   • All planning considerations are met. Refer to the *hp StorageWorks product in a SAN environment: planning guide for director 2/64, edge switch 2/16, and edge switch 2/32*.

3. Verify that all FRUs are installed as ordered.

4. Verify that the SFP optical transceivers are installed as required for your installation.

5. Connect the U.S. or country-specific (optional) AC power cords to the right (**PS0**) and left (**PS1**) receptacles at the rear of the chassis.

> ⚠ **WARNING: An HP-supplied power cord is provided for each switch power supply. To prevent electric shock when connecting the switch to primary facility power, use only the supplied power cords, and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.**

6. Connect the remaining ends of the AC power cords to separate facility power sources that provide single-phase, 120 to 240 volt alternating current (VAC) current. This provides power redundancy.

7. Turn on the power. Two power switches are on the back of the unit. Turn on both switches. The unit powers on and performs power-on self-tests (POSTs). During POSTs:

    a. The green power (**PWR**) LED on the front panel turns *On*.

    b. The amber system error (**ERR**) LED on the front panel flashes momentarily while the switch is tested.

    c. The green LEDs associated with the Ethernet port flashes momentarily while the port is tested.

    d. The green and amber LEDs associated with the ports flash momentarily while the ports are tested.

8. After successful POST completion, the green power (**PWR**) LED remains ON and all other front panel LEDs turn OFF.

9. If a POST error or other malfunction occurs, refer to the *hp StorageWorks edge switch 2/32 service manual* to isolate the problem.

Rack-Mount Installation

To install the switch in a customer-supplied equipment rack, refer to the *hp StorageWorks edge switch rack mount kit installation instructions*. The installation instructions are located on the *hp StorageWorks edge switch 2/32 documentation CD*.

Task 3: Configure Network Information

The edge switch 2/32 is delivered with the following default network addresses:

- **MAC address**—the media access control (MAC) address is programmed into FLASH memory on the CTP card at the time of manufacture. The MAC address is unique for each switch, and should not be changed. The address is in xx.xx.xx.xx.xx.xx format, where *xx* is a hexadecimal pair.

NOTE: References to the CTP in this manual are to the control processor logic contained on the switch motherboard. If an event occurs that indicates the CTP as faulty, replacement of the switch assembly is required.

- **IP address**—the factory preset default internet protocol (IP) address is **10.1.1.10.** The default IP address is also **10.1.1.10**.

    If **Reset Configuration** is selected from the *Product Manager* application, the switch resets to the default address of **10.1.1.10**.

    If multiple switches are installed on the same LAN, each switch (and the HAFM server) must have a unique IP address. One switch can use the factory-set address, but the addresses of the remaining switches must be changed.

NOTE: If you have enabled additional port function with the HP Flexport Feature since the switch shipped from the factory, resetting the configuration will return this feature to the factory default of only 16 ports enabled. You must re-enable the additional ports using the Configure Feature Key dialog box (see).

⚠ **WARNING: This operation resets all configuration including any optional features that have been installed. You will need to re-enter your feature key to enable all optional features after resetting the configuration parameters.**

- **Subnet mask**—the default subnet mask is **255.0.0.0**. If the switch is installed on a complex public LAN with one or more routers, the address may require change.

- **Gateway address**—the default gateway address is **0.0.0.0**. If the switch is installed on a dedicated LAN with no connection through a router, the address does not require change. If the switch is installed on a public LAN (corporate intranet), the gateway address must be changed to the address of the corporate intranet's local router.

Verify the type of LAN installation with the customer's network administrator. If one switch is installed on a dedicated LAN, network addresses do not require change.

If multiple switches are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme. The following tools are required:

- A maintenance terminal (desktop or notebook PC) with:

  — The Microsoft Windows 98, Windows 2000, Windows XP, or Windows Millennium Edition operating system installed.

  — RS-232 serial communication software (such as ProComm Plus or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.

  Note that the HAFM server may be used for this function and that HyperTerminal is included in Windows 2000 provided in the HAFM server as a windows 2000 application.

- An asynchronous RS-232 null modem cable (provided with the switch).

Perform the following steps to change a switch's IP address, subnet mask, or gateway address:

1. Remove the protective metal plate from the 9-pin maintenance port at the rear of the switch (a phillips-tip screwdriver is required). Connect the 9-pin end of the RS-232 null modem cable to the port.

2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.

3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays. Refer to operating instructions shipped with the PC.

NOTE: Steps 4-13 describe changing network addresses using the HyperTerminal serial communication software.

---

4. Choose **Start** > **Programs** > **Accessories** > **Communications** >**HyperTerminal**. The **Connection Description** dialog box displays, as shown in Figure 2–1.
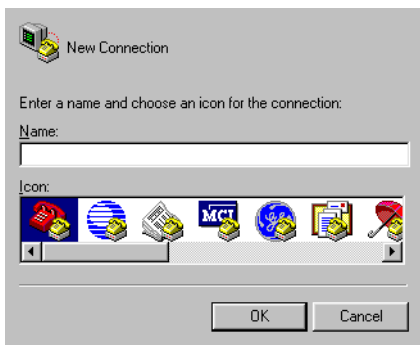
Figure 2–1: Connection Description dialog box

5. Type edge switch 2-32 in the **Name** field and click **OK**. The **Connect To** dialog box displays, as shown in Figure 2–2.

Figure 2–2: Connect To dialog box

6. Ensure the **Connect using** field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click **OK**. The **Port Settings** dialog box displays, as shown in Figure 2–3.
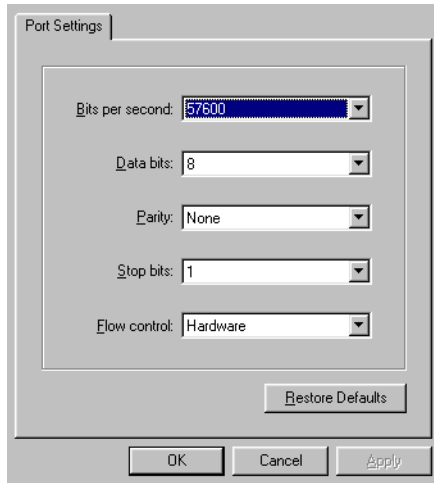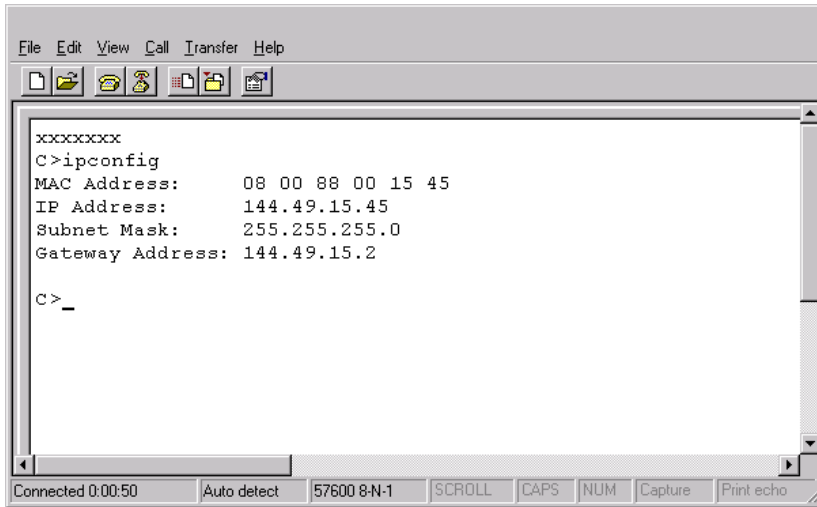
Figure 2–3: Port Settings dialog box

7. Configure the **Port Settings** parameters as follows:

   — **Bits per second**—57600

   — **Data bits**—8

   — **Parity**—None

   — **Stop bits**—1

   — **Flow control**—Hardware

   When the parameters are set, click **OK**. The **HyperTerminal** window displays.

8. At the **>** prompt, type the user-level password (the default is password) and press **Enter**. The password is case sensitive. The **HyperTerminal** window displays with a C**>** prompt at the top of the window, as shown in Figure 2–4.

Figure 2–4: HyperTerminal window

9. At the `C>` prompt, type `ipconfig` and press **Enter**. The **HyperTerminal** window displays with configuration information listed as follows:

   — **MAC Address**

   — **IP Address** (default is `10.1.1.10`, factory preset is `10.1.1.10`)

   — **Subnet Mask** (default is `255.0.0.0`).

   — **Gateway Address** (default is `0.0.0.0`)

   Only the **IP Address**, **Subnet Mask**, and **Gateway Address** fields are configurable.

10. Change the IP address, subnet mask, and gateway address as directed by the customer's network administrator. To change switch network addresses, type the following at the `C>` prompt and press **Enter**.

    `ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz`

    The IP address is always xxx.xxx.xxx.xxx, the subnet mask is always yyy.yyy.yyy.yyy, and the gateway address is always zzz.zzz.zzz.zzz, where the octets *xxx*, *yyy*, and *zzz* are decimals from zero through 255. If a network address is to remain unchanged, type the current address in the respective field.

    When the new network addresses are configured at the switch, the message `Request completed OK` displays at the bottom of the **edge switch 2/32 — HyperTerminal** window.

11. Choose **Exit** from the **File** menu to close the *HyperTerminal* application. A message box displays, as shown in Figure 2–5.
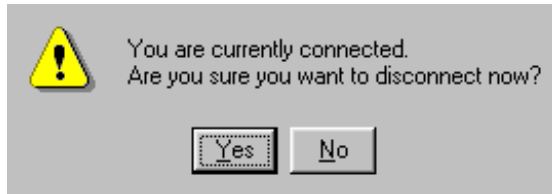
Figure 2–5: Disconnect Now dialog box

12. Click **Yes**. A message box displays, as shown in Figure 2–6.
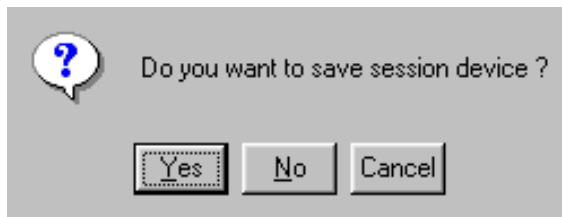
Figure 2–6: Save Session dialog box

13. Click **No** to exit and close the *HyperTerminal* application.

14. Power off the maintenance terminal:

    a. Choose **Start** > **Shut Down**. The **Shut Down Windows** dialog box displays.

    b. At the **Shut Down Windows** dialog box, choose **Shut down the Computer** and click **Yes** to power off the PC.

15. Disconnect the RS-232 null modem cable from the switch and the maintenance terminal. Replace the protective plate over the maintenance port.

Task 4: LAN-Connect the Switch

Connect the switch to the customer-supplied Ethernet LAN segment or the HP-supplied Ethernet hub.

To connect the desktop or rack-mounted switch to the Ethernet LAN segment:

1. Connect one end of the Ethernet patch cable (supplied with the switch) to the RJ-45 connector (labeled **10/100**) on the left front of the chassis.

2. Connect the remaining end of the Ethernet cable to the LAN as follows:

   a. If the switch is installed on a customer-supplied LAN segment, connect the cable to the LAN as directed by the customer's network administrator.

   b. If the switch is installed on the HP-supplied Ethernet hub, connect the cable to any available port on the hub.

3. Perform one of the following steps:

   • If an HAFM server or customer-supplied server platform is delivered and available, the Ethernet LAN segment does not require connection to the internet. Go to "Task 5: HAFM Server (Optional)" on page 2–12.

   • If an HAFM server is not available and the switch is managed through the EWS interface, attach the Ethernet LAN segment to an internet connection and go to "Task 15: Configure the Switch from the Embedded Web Server (Optional)" on page 2–51.

Task 5: HAFM Server (Optional)

To run HAFM software, you must set up and configure the HP OmniBook 6000/62000 notebook PC to function as an HAFM server.
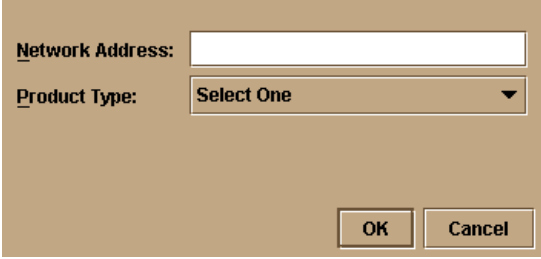
Refer to the *hp StorageWorks HAFM server installation guide* for instructions on:

• Setting up the HAFM server

• Connecting the HAFM server to the LAN

• Configuring the network addressing for the HAFM server

• Setting HAFM server date and time

• Creating HAFM user names and passwords

Task 6: Configure the Switch to the HAFM Application

To manage a new switch, it must be identified to the *HAFM* application. To identify the new switch:

1. Right-click in a blank area of the **Product View** page and select **New** or click **Product** on the menu bar and choose **New**. The **New Product** dialog box displays, as shown in Figure 2–7.

Figure 2–7: New Product dialog box

2. Type the IP address or DNS host name of the switch (determined by the customer's network administrator).

3. Select **edge-32** from the **Product Type** field and click **OK**. A new switch icon displays at the **Product View** page.

4. Repeat step 1 through step 3 for each new switch.

Task 7: Record or Verify HAFM Server Restore Information

Configuration information must be recorded to restore the HAFM server in case of hard drive failure. The Windows 2000 operating system and the HAFM and Edge Switch 2/32 *Product Manager* application must also be restored. Refer to the *hp StorageWorks edge switch 2/32 service manual* for instructions.

To record or verify HAFM server configuration information refer to the *hp StorageWorks HAFM server installation guide* for instructions.

Task 8: Verify Switch-to-HAFM Server Communication

Communication must be verified between the switch and the HAFM server (*High Availability Fabric Manager* and *Product Manager* applications). To verify switch-to-server communication:

1. At the Windows 2000 desktop, click HAFM at the task bar (bottom of the desktop) to maximize the **Product View** page.

2. At the **Product View** page, inspect the shape and color of the symbol behind the Edge Switch 2/32 icon. Table 2–2 explains operational states and associated symbols.

Table 2–2: Switch Operational States and Symbols

Operational State	Symbol
Operational—switch-to server communication is established, the switch is operational, and no failures are indicated. Go to "Task 11: Set Switch Date and Time" on page 2–21.	
Degraded—switch-to server communication is established, but the switch is operating in degraded mode and requires service. This condition is typical if a port or redundant FRU fails. Go to step 3.	
Failed—switch-to server communication is established, but the switch failed and requires immediate service. Go to step 3.	
Status Unknown—the switch status is unknown because of a network communication failure between the switch and HAFM server. Go to step 3.	

3. Double-click the **switch** icon. The **Hardware View** page for the selected switch displays, as shown in Figure 2–8. In the example, FRU failures are indicated by *Flashing* red and yellow diamonds, and switch degradation is indicated by the yellow triangle at the alert panel.
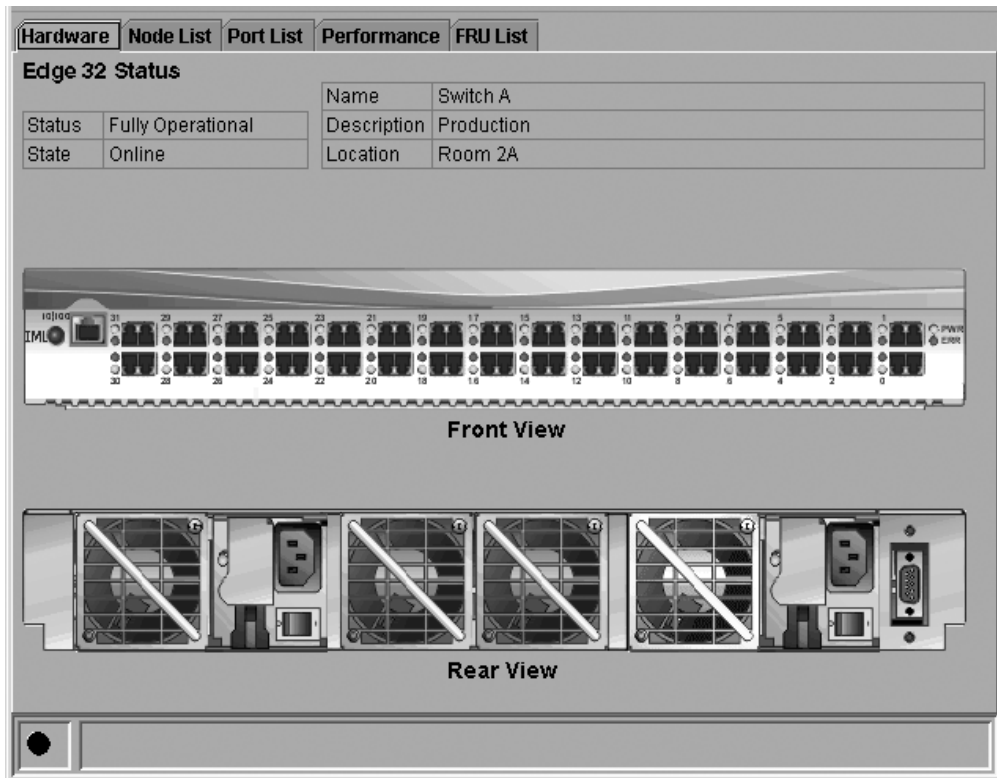
Figure 2–8: Switch Hardware View page

4. Inspect switch status at the **Hardware View** page and perform one of the following steps:

   a. If the switch displays operational (no FRU alert symbols and a green circle at the alert panel), go to "Task 11: Set Switch Date and Time" on page 2–21.

   b. If switch operation displays degraded or a switch failure is indicated (FRU alert symbols and a yellow triangle or red diamond at the alert panel), refer to the *hp StorageWorks edge switch 2/32 service manual* to isolate the problem.

Task 9: Configure Feature Key (Optional)

Perform this task to display or install operating features that are available as customer-specified options. Available features include the:

• Open systems management server (OSMS)

- Fiber connection (FICON) management server (FMS)

These features allow open systems or FICON host control of the switch and are mutually exclusive. Only one of these features can be installed at a time.

Features are enabled through a feature key that is encoded to work with the serial number of a unique switch. A feature key is a case-sensitive alphanumeric string with dashes every four characters.

Configure HP Flexport Technology Feature Key

This feature key enables additional port function. The factory default settings enable 16 of the 32 ports, and this feature key enables additional ports. Until this feature is enabled the additional ports will display as Not Installed in the Port Operational State window of the Hardware View and Port List View pages. See Chapter 3 for instructions on configuring this feature key and on upgrading the number of ports.

Configure OSMS Feature Key

NOTE: HP does not support OSMS.

Perform this procedure to configure the OSMS feature key. This feature enables host control of the switch from an open-systems interconnection (OSI) device attached to a switch port. The device communicates with the switch through the Fibre Channel common transport (FC-CT) protocol.

To configure the OSMS feature key:

1. Set the switch offline.

2. At the **Hardware View** page for the selected switch, choose **Configure** > **Features**. The **Configure Feature Key** dialog box displays, as shown in Figure 2–9.
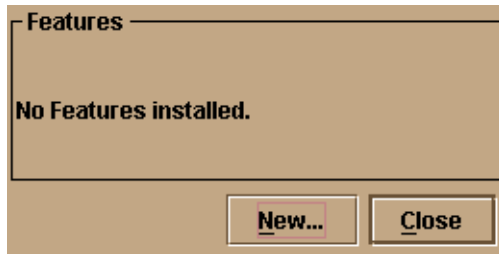
Figure 2–9: Configure Feature Key dialog box

3. Click **New**. The **New Feature Key** dialog box displays, as shown in Figure 2–10.

Figure 2–10: New Feature Key dialog box

4. Type the OSMS feature key (case-sensitive xxxx-xxxx-xxxx-xx format) and click **OK**. The **Enable Feature Key** dialog box displays, as shown in Figure 2–11.
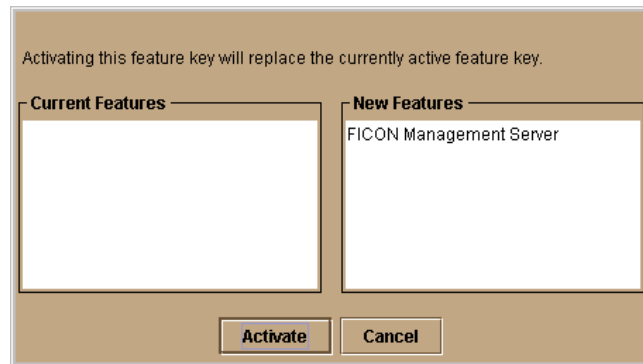
Figure 2–11: Enable Feature Key dialog box

5. Click **Activate** to enable the OSMS feature key. When the feature key is enabled, the switch performs an IPL, but *is not* automatically set to open systems operating mode.

Configure FMS Feature Key

Perform this procedure to configure the FMS feature key. This feature key enables host control of the switch from an IBM System/390 or zSeries 900 Parallel Enterprise server attached to a switch port. The server communicates with the switch through a FICON channel.

S/390 Only

To configure the FMS feature key:

1. Set the switch offline.

2. At the **Hardware View** page for the selected switch, choose **Configure** > **Features**. The **Configure Feature Key** dialog box displays, as shown in Figure 2–12.
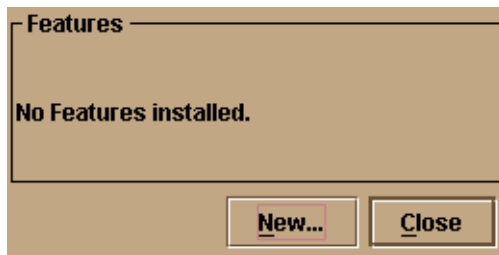
Figure 2–12: Configure Feature Key dialog box

3. Click **New**. The **New Feature Key** dialog box displays, as shown in Figure 2–13.

Figure 2–13: New Feature Key dialog box

4. Type the FMS feature key (case-sensitive xxxx-xxxx-xxxx-xx format) and click **OK**. The **Enable Feature Key** dialog box displays.

5. Click **Activate** to enable the FMS feature key, as shown in Figure 2–14. When the feature key is enabled, the switch performs an IPL and is automatically set to S/390 operating mode.
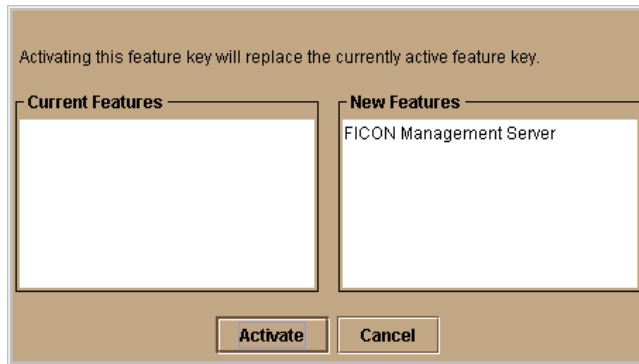
Figure 2–14: Activate FMS feature key

Task 10: Configure OSMS or FICON Management Server (Optional)

Perform this task to configure the open systems management server or FICON management server. Only one management server can be configured at a time.

Configure OSMS

Perform this procedure to configure the open systems management server and enable OSI host control of the switch. Implementing host control requires installation of a SAN management application on the OSI server. Management applications include Veritas SANPoint Control (Version 1.0 or later), or Tivoli NetView (Version 6.0 or later).

To configure the open systems management server:

1. At the **Hardware View** page for the selected switch, choose **Configure > Management Server**. The **Configure Open Systems Management Server** dialog box displays, as shown in Figure 2–15.
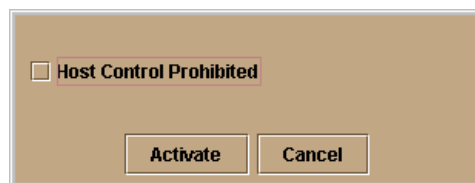
Figure 2–15: Configure Open Systems Management server dialog box

2. Allow or prohibit host (OSI server) control by selecting **Host Control Prohibited**. If a check mark displays, host control is prohibited.

3. Click **Activate** to enable a change and allow or prohibit open systems host control.

Configure FMS

Perform this procedure to configure the FICON management server and enable FICON host control of the switch. Implementing host control requires installation of System Automation for Operating System/390 (SA OS/390), version 1.2 or later.

S/390 Only

To configure the FICON management server:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **Management Server**. The **Configure FICON Management Server** dialog box displays, as shown in Figure 2–16.

Figure 2–16: Configure FICON Management server dialog box

2. Enable or disable the following options by clicking the associated check box:

   • **Switch Clock Alert Mode**—this option enables or disables a warning message that displays if the switch is set to periodically synchronize date and time with the HAFM server (see "Task 11: Set Switch Date and Time" on page 2–21). Synchronizing date and time with the HAFM server may conflict with the date and time set from the attached host. If a check mark displays, clock alert mode is enabled.

   • **Programmed offline state control**—this option enables or disables host (S/390 or zSeries 900) ability to set the switch offline state. If a check mark displays, control is enabled.

   • **Host Control Prohibited**—this option allows or prohibits host (S/390 or zSeries 900) control of the switch. If a check mark displays, host control is prohibited.

- **Active = Saved**—when this option is enabled, the active configuration of logical port addresses is used when the IPL configuration file is updated. If a check mark displays, the **Active = Saved** option is enabled.

3. Select the appropriate country code page from the following **Code Page** list box, as shown in Table 2–3.

Table 2–3: Code Page Choices

Code Page Name	Code Page
United States/Canada	00037
Germany/Austria	00273
Brazil	00275
Italy	00280
Japan	00281
Spain/Latin America	00284
United Kingdom	00285
France	00297
International #5	00500

4. Click **Activate** to enable changes and allow or prohibit FICON host control.

Task 11: Set Switch Date and Time

The Edge Switch 2/32 Product Manager log entries are stamped with the date and time received from the switch. To set the effective date and time for the switch:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **Date/Time**. The **Configure Date and Time** dialog box displays, as shown in Figure 2–17.

The switch date and time can be set manually, or set to be periodically updated by the *HAFM* application (the switch and *HAFM* application synchronize at least once daily).
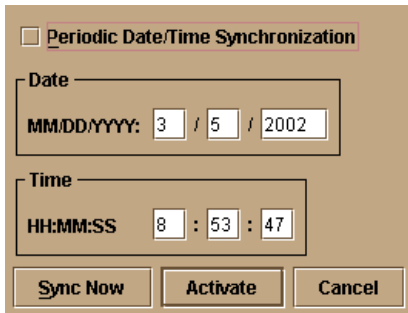
Figure 2–17: Configure Date and Time dialog box

Set Date and Time Manually

To set the switch date and time manually:

1. At the **Configure Date and Time** dialog box, click **Periodic Date/Time Synchronization** to deselect the option (no check mark in the box). The greyed out **Date and Time** fields activate.

2. Click the **Date** fields that require change, and type numbers in the following ranges:

   Month (MM): 1 through 12
   Day (DD): 1 through 31
   Year (YY): greater than 1980

3. Click the **Time** fields that require change, and type numbers in the following ranges:

   Hour (HH): 0 through 23
   Minute (MM): 0 through 59
   Second (SS): 0 through 59

4. Click **Activate** to set the switch date and time and close the **Configure Date and Time** dialog box.

Periodically Synchronize Date and Time

To set the switch to periodically synchronize date and time with the *HAFM* application:

1. Click **Periodic Date/Time Synchronization** to select the option (check mark in the box). The **Date and Time** fields are greyed out and not selectable. Perform one of the following options:

   - Click **Activate** to enable synchronization and close the **Configure Date and Time** dialog box. The switch date and time synchronize with the *HAFM* application date and time at the next update period (at least once daily).

   - Click **Sync Now** to synchronize the switch and *HAFM* application immediately. The **Date and Time Synced** dialog box displays, as shown in Figure 2–18.
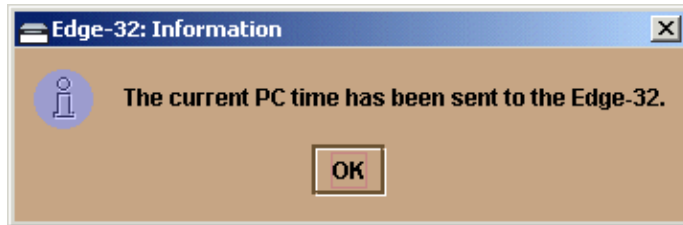
Figure 2–18: Date and Time Synced dialog box

2. Click **OK** to synchronize the date and time and close the **Date and Time Synced** dialog box, then click **Activate** to enable synchronization and close the **Configure Date and Time** dialog box.

Task 12: Configure the Edge Switch 2/32 Product Manager Applications

Selectively perform the following configuration tasks for the Edge Switch 2/32 *Product Manager* application according to the customer's installation requirements. For additional information, refer to the *hp StorageWorks edge switch 2/32 product manager user guide*.

- Identify the switch to the *HAFM* application.

- Configure switch operating mode (open systems or S/390).

- Configure switch operating parameters.

- Configure switch ports.

S/390 Only

- Configure logical port addresses.

- Configure SNMP trap message recipients.

- Configure and enable e-mail notification.

- Enable call-home notification.

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person for the *HAFM* application. The information displays in multiple dialog boxes throughout the application. In addition, the *Name*, *Location*, and *Contact* variables configured at the **Configure Identification** dialog box correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. These variables are used by SNMP management workstations when obtaining data from managed switches.

To configure the switch identification:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **Identification**. The **Configure Identification** dialog box displays, as shown in Figure 2–19.

Name:	Undefined	☐ **Set Name As Nickname**
Description:		
Location:		
Contact:		
	Activate	**Cancel**

Figure 2–19: Configure Identification dialog box

    a. Type a switch name of 24 alphanumeric characters or less in the **Name** field. Each switch should be configured with a unique name.

       If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network DNS host name. For example, if the DNS host name is hpes232.hp.com, enter `hpes232`.

    b. Click **Set Name as Nickname** and add a check mark if you want to use the name in the name field as the nickname for the switch's WWN. The nickname will display instead of the WWN in Product Manager views.

    c.   Type a switch description of 255 alphanumeric characters or less in the **Description** field.

    d.   Type the switch's physical location (255 alphanumeric characters or less) in the **Location** field.

    e.   Type the name of a contact person (255 alphanumeric characters or less) in the **Contact** field.

2.   Click **Activate** to configure the switch identification and close the dialog box.

Configuring the Switch

Configuring Switch Operating Parameters

Use the procedures in this section to set parameters on the switch for fabric operation through the **Configure Switch Parameters** dialog box. These operating parameters are stored in NV-RAM on the switch.

1.   The switch must be offline to change **Preferred Domain ID** and **Operating Mode** parameters. If it is not and you activate values in this dialog box, a dialog box displays prompting you to set the unit offline.

    ⚠   **CAUTION:** Setting the switch offline terminates all Fibre Channel connections.

To set the unit offline.

    a.   Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.

    b.   Click **Set Offline**. A warning box displays asking you to confirm the offline state.

    c.   Click **OK**.

2.   Choose **Configure > Operating Parameters > Switch Parameters**. The **Configure Switch Parameters** dialog box displays, as shown in Figure 2–20.
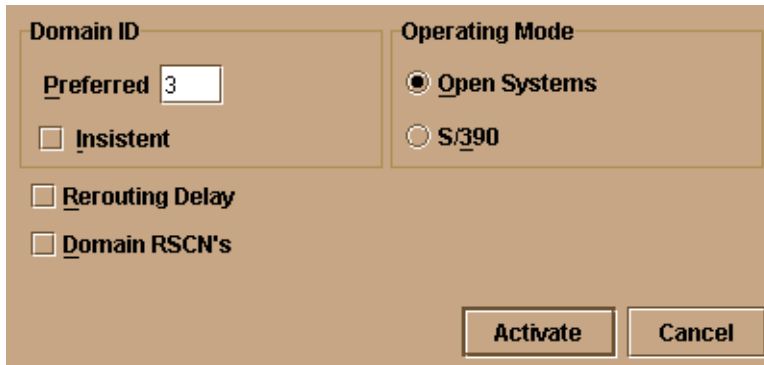
Figure 2–20: Configure Switch Parameters dialog box

Ordinarily, you do not need to change values in this dialog box from their defaults. The only exception is the **Preferred Domain ID**. Change this value if the switch will participate in a multiswitch fabric.

1. Use information under "Switch Parameters" to change settings as required for parameters in this dialog box.

2. After you change settings, click the **Activate** button.

Switch Parameters

Configure the following parameters as required by your fabric.

Domain ID

The domain identification is a value between 1 and 31 that provides a unique identification for the switch in a fabric. An Edge Switch cannot contain the same domain ID as another switch or their E_Ports will segment when they try to join.

In the **Configure Switch Parameters** dialog box, a field is provided to enter a preferred domain ID and a check box is provided to enable this ID as an insistent domain ID.

Preferred

NOTE: To change this value, you must first set the switch offline. Choose Set Online State from the Maintenance menu to display the Set Online State dialog box, then click the Set Offline button. Be sure to set the switch back online after you change this value.

Use this field to set the a unique domain ID for the switch. The default value is 1. Set a value between 1 and 31. When a switch comes online with a preferred ID, it requests an ID from the fabric's principal switch (indicating its preferred value as part of the request). If the requested domain ID is not allocated to the fabric, the domain ID is assigned to the requesting switch. If the requested domain ID is already allocated, an unused domain ID is assigned. Note that you must set the switch offline before you can change to the preferred domain ID.

The preferred domain ID must be unique for each director and switch in a fabric. If two switches or directors have the same preferred domain ID, the E_Ports segment, causing the fabric to segment.

For more information on domain ID, refer to the section on domain ID assignment for multiswitch fabrics in the *HP StorageWorks Products in a SAN Environment — Planning Manual* for details.

Insistent

This option is not supported unless the SANtegrity feature is installed. Click the check box to remove or add a check mark. The default state is disabled (no check mark).

When a check mark displays, the domain ID configured in the **Preferred Domain ID** field will become the active domain identification when the fabric initializes. See the following notes:

- This option is required if High Availability Fabric Manager (HAFM) is enabled.

- If you enable Insistent Domain while the switch or director is online, the Preferred Domain ID will change to the current active domain ID if the IDs are different.

$\triangle$ **CAUTION:** If a switch with a duplicate domain ID exists in the fabric, both switches' E_Ports will segment when they try to join.

Rerouting Delay

Placing a check mark in the check box to the left of the **Rerouting Delay** option enables rerouting delay. This option is only applicable if the configured switch is in a multiswitch fabric. The default state is disabled.

Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the **Configure Fabric Parameters** dialog box. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path.

NOTE: This option is required if High Availability Fabric Manager (HAFM) is enabled.

Domain RSCNs

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. Note that this option is required if High Availability Fabric Manager (HAFM) is enabled.

Operating Mode

NOTE: To change this value, you must first set the switch offline. Select Set Online State from the Maintenance menu to display the Set Online State dialog box, then click the Set Offline button. Be sure to set the switch back online after you change this value.

Click either the S/390 or Open Systems radio buttons:

- If the FICON Management Server feature is enabled, the default mode will be S/390. The operating mode cannot be changed to Open Systems with the FICON Management Server feature enabled. Typically, S/390 mode is used when attaching an IBM S/390 Parallel Enterprise or IBM zSeries server to the switch and implementing inband switch management through a Fibre Connection (FICON) channel.

• Use **Open Systems** mode for all other (non-FICON) Fibre Channel environments.

Configure Fabric Operating Parameters

Use procedures in this section to set parameters on the switch for fabric operation through the **Configure Fabric Parameters** dialog box. These operating parameters are stored in NV-RAM on the switch.

1. The switch must be offline to change parameters in this dialog box. If it is not and you activate values, a dialog box displays prompting you to set the unit offline.

   $\triangle$ **CAUTION:** Setting the switch offline terminates all Fibre Channel connections.

   To set the unit offline:

   a. Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.

   b. Click **Set Offline**. A warning box displays asking you to confirm the offline state.

   c. Click **OK**.

2. Choose **Configure > Operating Parameters > Fabric Parameters** from the **Product Manager** window. The **Configure Fabric Parameters** dialog box displays, as shown in Figure 2–21.
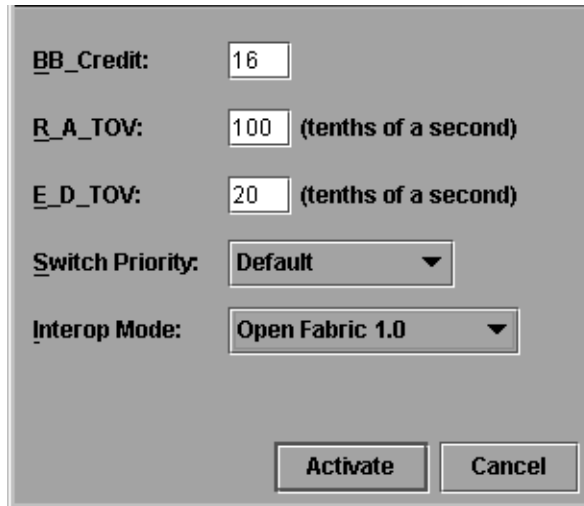
Figure 2–21: Configure Fabric Parameters dialog box

NOTE: Ordinarily, you do not need to change values in this dialog box from their defaults. The only exception is the Preferred Domain ID. Change this value if the switch will participate in a multiswitch fabric.

3. Use information under "Fabric Parameters" to change settings as required for parameters in this dialog box.

4. After you change settings, click the **Activate** button.

5. Back up the configuration data when you are finished configuring the switch.

Fabric Parameters

Configure the following parameters as required by your fabric.

BB_Credit

Configure the switch to support buffer to buffer credit (BB_Credit) from 1 through 60. This is the value used for all ports, except those configured for extended distance buffering (10-100 km). The default value is 16. For a description of the buffer-to-buffer credit, refer to the industry specification, *Fibre Channel Physical and Signaling Interface*.

R_A_TOV

Configure resource allocation time-out value (R_A_TOV) in tenth-of-a-second increments. This variable works with the error detect time-out value (E_D_TOV) variable to control the switch's behavior when an error condition occurs. Resources are allocated to a circuit when errors are detected and are not released for reuse until the time set by the R_A_TOV value expires. The default value is 100 tenths (10 seconds). Set a value between 10 tenths and 1200 tenths (1 through 120 seconds).

NOTE: Set the same value for R_A_TOV on all directors and switches in a multiswitch fabric. If the value is not the same on all units, the fabric segments. Also, the value for R_A_TOV must be greater than the value configured for E_D_TOV.

E_D_TOV

Adjust the E_D_TOV in tenth-of-a-second increments. An error condition occurs when an expected response is not received within the time limit set by this value. The default value is 20 tenths (2 seconds). Set a value between 2 tenths through 600 tenths (.2 through 60 seconds).

NOTE: Set the same value for E_D_TOV on all switches and directors in a multiswitch fabric. If the value is not the same, the fabric segments.

Switch Priority

Setting this value determines the principal switch for the multiswitch fabric. Choose **Principal** (highest priority), **Default**, or **Never Principal** (lowest priority) from the **Switch Priority** drop-down list.

Setting these priority values determines the principal switch selected for the multiswitch fabric. For example, if you have three switches in the fabric and set one as **Principal**, one as **Default**, and one as **Never Principal**, the unit set to **Principal** becomes the principal switch in the fabric.

If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest WWN becomes the principal switch. Following are some examples of principal switch selection when switches have these settings:

- If you have three switches and set all to **Default**, the switch with the lowest WWN becomes the principal switch.

- If you have three switches and set two to **Principal** and one to **Default**, the switch with the **Principal** setting that has the lowest WWN becomes the principal switch.

- If you have three switches and set two to **Default** and one to **Never Principal**, the switch with the **Default** setting and the lowest WWN becomes the principal switch.

At least one switch in a multiswitch fabric needs to be set as **Principal** or **Default**. If all of the switches are set to **Never Principal**, all of the interswitch links (ISLs) will segment. If all but one switch is set to **Never Principal** and the switch that was principal goes offline, then all of the other ISLs will segment.

NOTE: We recommend you leave the switch priority setting as Default. If you are considering setting this value to something other than default, refer to the section on principal switch selection for multiswitch fabrics in the HP StorageWorks Products in a SAN Environment — Planning Manual for details.

In, for example, the audit log, you may notice that the **Principal** setting maps to a number code of 1, **Default** maps to a number code of 254, and **Never Principal** maps to a number code of 255. The number codes of 2 — 253 are not currently in use.

Interop Mode

Select the following option:

- Open Fabric 1.0. Select this mode if the fabric contains HP directors and switches, as well as other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

Configure Ports (Open Systems Mode)

If the switch is set to open systems mode, perform this procedure to define Fibre Channel port names, configure ports as blocked or unblocked, enable extended distance operation and link incident (LIN) alerts configure port binding, and define port types.

To configure switch ports:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **Ports**. The **Configure Ports** dialog box (open systems mode) displays.

   a. Select a blank **Name** field and type a descriptive port name of 24 or fewer alphanumeric characters. Use a name that reflects the device connected to the port.

b. Click **Blocked** check box to block or unblock a port. A check mark in the box indicates the port is blocked. Blocking the port prevents the attached device from communicating with the switch. A blocked port continuously transmits the offline sequence (OLS), as shown in Figure 2–22.

Port #	Name	Blocked	10-100 km	LIN Alerts	Type	Speed	Port Binding
0		☐	☐	☑	G_PORT	1 Gb/sec	☐
1		☐	☐	☑	G_PORT	1 Gb/sec	☐
2		☐	☐	☑	G_PORT	2 Gb/sec	☐
3		☐	☐	☑	G_PORT	1 Gb/sec	☐
4		☐	☐	☑	G_PORT	1 Gb/sec	☐
5		☐	☐	☑	G_PORT	1 Gb/sec	☐
6		☐	☐	☑	G_PORT	2 Gb/sec	☐
7		☐	☐	☑	G_PORT	1 Gb/sec	☐
8		☐	☐	☑	G_PORT	1 Gb/sec	☐
9		☐	☐	☑	G_PORT	1 Gb/sec	☐
10		☐	☐	☐	G_PORT	2 Gb/sec	☐
11		☐	☐	☑	G_PORT	1 Gb/sec	☐
12		☐	☐	☑	G_PORT	1 Gb/sec	☐
13		☐	☐	☑	G_PORT	1 Gb/sec	☐
14		☐	☐	☐	G_PORT	2 Gb/sec	☐
15		☐	☐	☑	G_PORT	1 Gb/sec	☐

Figure 2–22: Configure Ports dialog box (open systems mode)

c. Click **10-100 km** to enable extended distance buffering for a port. A check mark in the box indicates extended distance operation up to 100 kilometers (through repeaters) is enabled.

d. Click **LIN Alerts** to enable or disable LIN alerts for a port. A check mark in the box indicates alerts are enabled. When the feature is enabled and an incident occurs on the link, an alert indicator (yellow triangle) displays at the Hardware View, Port List View, and Port Card View pages, and a message is sent to configured e-mail recipients. LIN alerts are enabled by default.

e. Select a **Type** field and choose generic port (**G_Port**), fabric port (**F_Port**), or expansion port (**E_Port**) from the list box.

f. Click the **Speed** field for a port. A **Speed** drop-down list displays. Choose 1 Gb/sec, 2 Gb/sec, or Navigate as the desired setting depending on the speed capability of the device to be plugged into the port.

> A right-click in the Speed column allows you to choose from a menu to set all ports to 1 Gb/sec, 2 Gb/sec, or Navigate.
>
> g. **Port Binding**—Click this check box to display a check mark and enable WWN binding for the port. This allows only a specific device to attach to the port. This device is specified by the WWN or nickname entered into the **Bound WWN** column. With the check box cleared, any device can attach to the port even if a WWN or nickname is specified in the **Bound WWN** column.
>
> or
>
> **Bound WWN**—Enter a world wide name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through the *Product Manager* application. The device with this WWN or nickname will have exclusive attachment to the port if **Port Binding** is enabled. If a valid WWN or nickname is not entered in this field, but the **Port Binding** check box is checked (enabled), then no devices can connect to the port. If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can connect to the port.

2. Use the vertical scroll bar as necessary to display additional port information rows (up to 32 ports).

3. Click **Activate** to save the configuration information and close the dialog box.

Configure Ports (S/390 Mode)

If the switch is set to S/390 mode, perform this procedure to enable extended distance operation and LIN alerts for Fibre Channel ports. Then continue to "Configure Port Addresses (S/390 Mode)" on page 2–36 to define port names, configure ports as blocked or unblocked, and define the control unit port (CUP).

S/390 Only

To configure switch ports:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **Ports**. The **Configure Ports** dialog box (S/390 mode) displays, as shown in Figure 2–23.

Port #	10-100 km	LIN Alerts	WWN Binding	Speed	Bound WWN
0	☐	☑	☑	**1 Gb/sec**	20:00:00:00:C9:00:00:00
1	☐	☑	☐	**1 Gb/sec**	20:01:00:60:48:00:00:00
2	☐	☑	☐	**1 Gb/sec**	20:02:00:00:C9:00:00:00
3	☐	☑	☑	**1 Gb/sec**	20:03:00:60:48:00:00:00
4	☐	☑	☐	**1 Gb/sec**	20:04:00:E0:69:00:00:00
5	☐	☑	☐	**1 Gb/sec**	20:05:00:00:C9:00:00:00
6	☐	☑	☑	**1 Gb/sec**	20:06:00:00:C9:00:00:00
7	☐	☑	☐	**1 Gb/sec**	20:07:00:60:48:00:00:00
8	☐	☑	☐	**1 Gb/sec**	20:08:08:00:20:00:00:00
9	☐	☑	☑	**1 Gb/sec**	20:09:00:60:48:00:00:00
10	☐	☑	☐	**1 Gb/sec**	20:0A:00:60:48:00:00:00
11	☐	☑	☐	**1 Gb/sec**	20:0B:00:00:C9:00:00:00
12	☐	☑	☑	**1 Gb/sec**	20:0C:08:00:20:00:00:00
13	☐	☑	☐	**1 Gb/sec**	20:0D:00:00:C9:00:00:00
14	☐	☑	☐	**1 Gb/sec**	20:0E:00:00:C9:00:00:00
15	☐	☑	☑	**1 Gb/sec**	20:0F:08:00:20:00:00:00
16	☐	☑	☐	**1 Gb/sec**	20:10:08:00:20:00:00:00
17	☐	☑	☐	**1 Gb/sec**	20:11:00:60:48:00:00:00
18	☐	☑	☑	**1 Gb/sec**	20:12:00:00:C9:00:00:00
19	☐	☑	☐	**1 Gb/sec**	20:13:08:00:20:00:00:00
20	☐	☑	☐	**1 Gb/sec**	20:14:00:E0:69:00:00:00
21	☐	☑	☑	**1 Gb/sec**	20:15:00:00:C9:00:00:00
22	☐	☑	☐	**1 Gb/sec**	20:16:00:00:C9:00:00:00
23	☐	☑	☐	**1 Gb/sec**	20:17:08:00:20:00:00:00

Activate   Cancel

Figure 2–23: Configure Ports dialog box (S/390 mode)

  a. Click **10-100 km** to enable extended distance buffering for a port. A check mark in the box indicates extended distance operation up to 100 kilometers (through repeaters) is enabled.

  b. Click **LIN Alerts** to enable or disable LIN alerts for a port. A check mark in the box indicates alerts are enabled. When the feature is enabled and an incident occurs on the link, an alert indicator (yellow triangle) displays at the Hardware View, Port List View, and Port Card View pages, and a message is sent to configured e-mail recipients. LIN alerts are enabled by default.

  c. **WWN Binding**—Click this check box to display a check mark and enable WWN binding for the port. This allows only a specific device to attach to the port. This device is specified by the WWN or nickname entered into the **Bound WWN** column. With the check box cleared, any device can attach to the port even if a WWN or nickname is specified in the **Bound WWN** column.

  d. Choose a port speed.

    e. **Bound WWN**—Enter a World Wide Name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through the *Product Manager* application. The device with this WWN or nickname will have exclusive attachment to the port if **WWN Binding** is enabled. If a valid WWN or nickname is not entered in this field, but the **WWN Binding** check box is checked (enabled), then no devices can connect to the port. If you enter a WWN or nickname in this field and do not place a check in the **WWN Binding** check box, the WWN or nickname will be stored, and all devices can connect to the port.

2. Use the vertical scroll bar as necessary to display additional port information rows (up to 64 ports).

3. Click **Activate** to save the configuration information and close the dialog box.

Configure Port Addresses (S/390 Mode)

If the switch is set to S/390 mode, perform this procedure to access the switch matrix and define Fibre Channel port names, configure ports as blocked or unblocked, and define the CUP name. Perform this procedure in conjunction with "Configure Ports (S/390 Mode)" on page 2–34.

To configure switch port addresses:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **Addresses** > **Active**. The **Configure Addresses — Active** dialog box displays, as shown in Figure 2–24.

Figure 2–24: Configure Addresses—Active dialog box

    a. Select a blank **Name** field and type a descriptive port name of 24 or fewer alphanumeric characters. Use a name that reflects the device connected to the port.

    b. Click **Blocked** to block or unblock a port. A check mark in the box indicates the port is blocked. Blocking the port prevents the attached device from communicating with the switch. A blocked port continuously transmits the offline sequence (OLS).

2. The yellow shaded area of the dialog box (matrix) represents a rectangular array of port addresses used to configure connections. The default state is an empty cell representing an allowed connection between two port addresses.

    a. Click a blank matrix cell to prohibit the connection of the two intersecting ports. A prohibited connection is indicated by a red circle with a slash in the cell.

    b. Click a prohibited matrix cell to clear the restriction and allow the connection of the two intersecting ports.

    c. Right-click a matrix cell to display a menu that provides the following port configuration selections:

- Prohibit or allow connections for an entire row (row **0C** is prohibited in the **Configure Addresses—Active** dialog box example),

- Prohibit or allow connections for all switch ports,

- Block or unblock all switch ports, or

- Clear connectivity restrictions for all switch ports.

3. At the **CUP Name** field, type a control unit port description of 24 or fewer alphanumeric characters (optional). The CUP is an internal switch port that communicates with channels to report errors and link initialization.

4. Perform one of the following to activate the configuration (without saving it), or save the configuration for later activation:

   - **Activate the Configuration**—click **Activate** to activate the configuration changes (without saving) and close the *Configure Addresses — Active* dialog box.

   - **Save the Configuration**—click **Save As**. The **Save Address Configuration As** dialog box displays, as shown in Figure 2–25.

Figure 2–25: Save Address Configuration As dialog box

   — At the **Name** field, type a configuration name of 8 or fewer alphanumeric characters.

   — At the **Description** field, type a configuration description of 24 or fewer alphanumeric characters.

   — Click **OK** to save the configuration in the address configuration library and close the **Save Address Configuration As** dialog box.

   — At the **Configure Addresses—Active** dialog box, click **Activate** to activate the configuration and close the dialog box, or click **Close** to close the dialog box.

Configure SNMP Trap Message Recipients

Perform this procedure to configure community names, write authorizations, and network addresses and for up to 12 SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs.

To configure SNMP trap recipients:

1. At the **Hardware View** page for the selected switch, choose **Configure** > **SNMP Agent**. The **Configure SNMP Agent** dialog box displays, as shown in Figure 2–26.

Figure 2–26: Configure SNMP Agent dialog box

   a. For each trap recipient to be configured, type a community name of 64 alphanumeric characters or less in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.

   b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change the HAFM server's *sysContact*, *sysName*, and *sysLocation* SNMP variables.

   c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 32 alphanumeric characters or less. It is recommended the IP address be used.

   d. The default user datagram protocol (UDP) port number for trap recipients is 162. Type a decimal port number in the associated **UDP Port Number** field to override the default.

2. To enable transmission of trap messages to configured SNMP management workstations, click **Enable Authorization Traps**. A check mark displays in the box when transmission is enabled, as shown in Figure 2–27.

Figure 2–27: Configure SNMP dialog box—Enable Authorization Traps
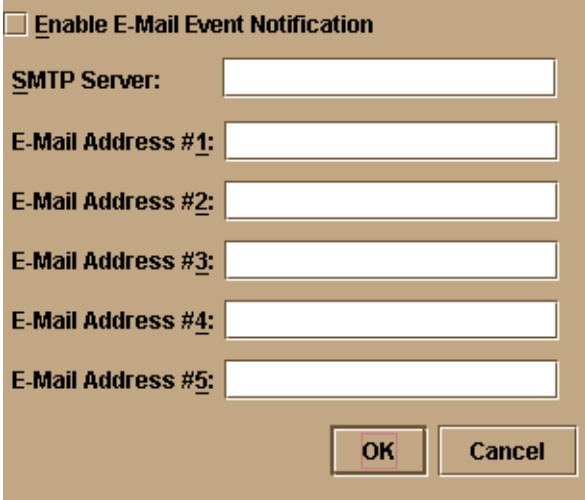
3. Click **Activate** to save the information and close the dialog box.

Configure and Enable E-mail Notification

Perform this procedure to configure and enable e-mail addresses and simple mail transfer protocol (SMTP) server addresses to receive e-mail notification of switch (and other managed product) events. The addresses must be configured at the *HAFM* application, then enabled. See "Task 13: Test Remote Notification (Optional)" on page 2–50 for instructions on testing this notification feature.

To configure and enable e-mail and SMTP server addresses:

1. At the **Product View** page, choose **Maintenance** > **Configure E-Mail**. The **Configure E-Mail** dialog box displays, as shown in Figure 2–28.

Figure 2–28: Configure E-Mail dialog box

    a. Type the IP address or DNS host name of the SMTP server in the **SMTP server** field. Use 64 alphanumeric characters or less. It is recommended the IP address be used.

    b. For the **E-Mail Addresses** fields, type the e-mail addresses of up to five recipients who should be informed of system events. Use 64 alphanumeric characters or less for each entry.

2. To enable e-mail transmission to configured addresses, click **Enable E-Mail Event Notification**. A check mark displays in the box when transmission is enabled.

NOTE: The enable function must also be activated for each switch through the Edge Switch 2/32 *Product Manager* application. E-mail notification can be active for some switches and inactive for others.

---

3. Click **OK** to save the information and close the dialog box.

4. Click the switch icon. The Hardware View page for the selected switch displays.

5. At the **Hardware View** page for the selected switch, choose **Maintenance** > **Enable E-Mail Notification**. A check mark displays in the check box to indicate e-mail notification for the switch is enabled, and the menu closes.

Configure and Enable Call-Home Features

There are two call-home features available, and only one is installed when the *HAFM* application is installed on the HAFM server. To learn more about configuring Call-Home features, refer to the *hp StorageWorks HAFM server installation guide*.

Configure Threshold Alerts

A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific switch ports or port types, (E_Ports or F_Ports).

You are notified of a threshold alert in four ways:

- An attention indicator (yellow triangle) that displays on the port in the **Hardware View** page.
- An attention indicator (yellow triangle) that displays in the **Alert** column of the **Port List View** page.
- An attention indicator (yellow triangle) that displays by the **Threshold Alerts** field in the **Port Properties** dialog box.
- Detailed threshold alert data is recorded in the *Threshold Alert Log*.

Choose **Configure** > **Threshold Alerts** to configure the following:

- Name for the alert.
- Type of threshold for the alert (Rx, Tx, or either).
- Active or inactive state of the alert.
- Threshold criteria:
    — Percent traffic capacity utilized. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value. For example the value of 50 means that the port's threshold is reached when throughput is 50% of capacity.
    — Time interval during which throughput is measured and alert notification can occur.
    — The time that the percentage of throughput capacity (% utilization) must exist during the set time interval before an alert generates.
- Ports for which you are configuring threshold alerts.

You can configure up to 16 alerts, and any number of alerts can be active at one time.

Procedures

Use the following procedures to create a new threshold alert, or to modify, activate, deactivate, or delete an alert.

Create New Alert
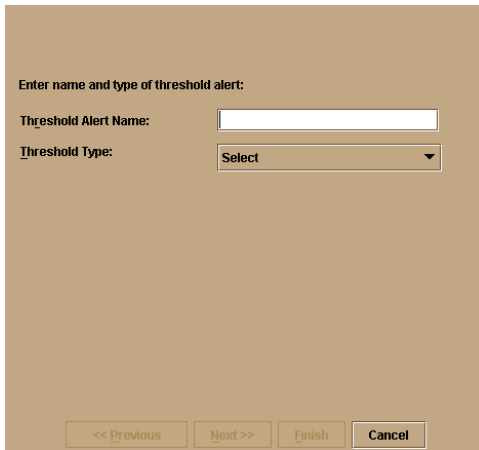
1. At the **Hardware View** for the selected switch, choose **Configure** > **Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays, as shown in Figure 2–29.

   If alerts are configured, they will display in table format showing the name of the alert, type of alert (Rx, TX, or Rx or Tx), and alert state (inactive or active).

Name	Type	State

New... Modify... View Delete Activate Deactivate **Close**
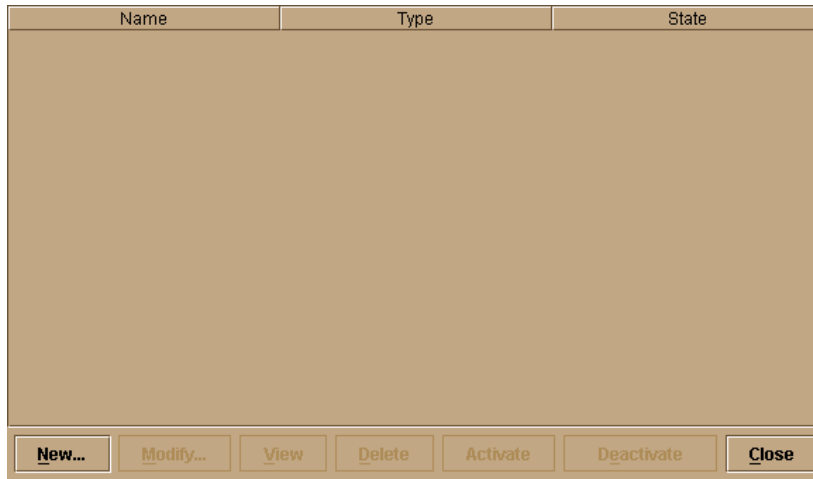
Figure 2–29: Configure Threshold Alerts dialog box
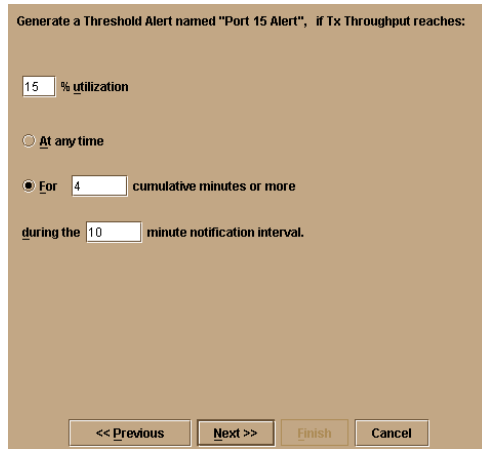
2. Click **New.** The **New Threshold Alert** dialog box displays, as shown in Figure 2–30.

Figure 2–30: New Threshold Alerts dialog box—first screen

3. Enter a name from one to 64 characters in length. All characters in the ISO Latin-1 character set, excluding control characters, are allowed.

4. Select one of the following options from the drop-down list under the **Name** field:

   • **Rx Throughput**. An alert will occur if the threshold set for receive throughput is reached.

   • **Tx Throughput**. An alert will occur if the threshold set for transmit throughput is reached.

   • **Rx or Tx Throughput**. An alert will occur if the threshold set for either receive or transmit throughput is reached.

5. Click **Next**. A new screen displays with additional parameters. The name configured for the alert displays at the top of the screen. Click **Previous** to return to the previous screen, as shown in Figure 2–31.

Generate a Threshold Alert named "Port 15 Alert", if Tx Throughput reaches:

[15]   % utilization

○ At any time

● For   [4]   cumulative minutes or more

during the [10]   minute notification interval.

[<< Previous]   [Next >>]   [Finish]   [Cancel]

Figure 2–31: New Threshold Alerts dialog box—second screen

6. Enter a percentage from 1 through 100 for **% utilization**. When throughput reaches this percentage of port capacity, a threshold alert will occur.

7. Enter the amount of cumulative minutes in which the **% utilization** should exist during the notification interval before an alert is generated. You can also select **At any time** if you want an alert to occur whenever the set **% utilization** is reached. The valid range is 1 to the interval set in step 8 (following).

8. Enter the interval in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.

9. Click **Next**. A new screen displays for selecting ports for the alerts, as shown in Figure 2–32.
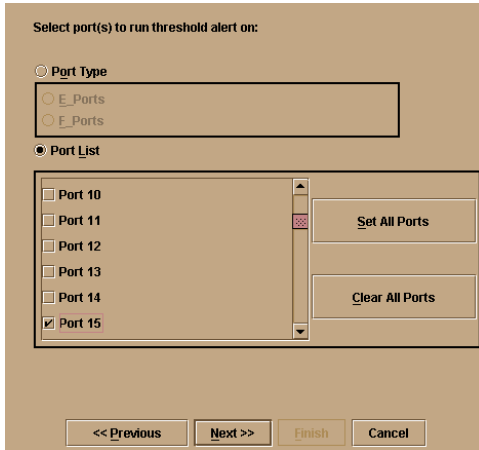
Figure 2–32: New Threshold Alerts dialog box—third screen

10. Either select **Port Type** or **Port List**.

    •   If you select **Port Type**, selecting either E_Ports or F_Ports will cause this alert to generate for all ports configured as E_Ports or F_Ports respectively.

    •   If you select **Port List**, you can select individual ports by clicking the check box by each port number or set all ports. Selecting **Set All Ports** places a check mark by each port number. Selecting **Clear All Ports** will clear the check marks by each port number.
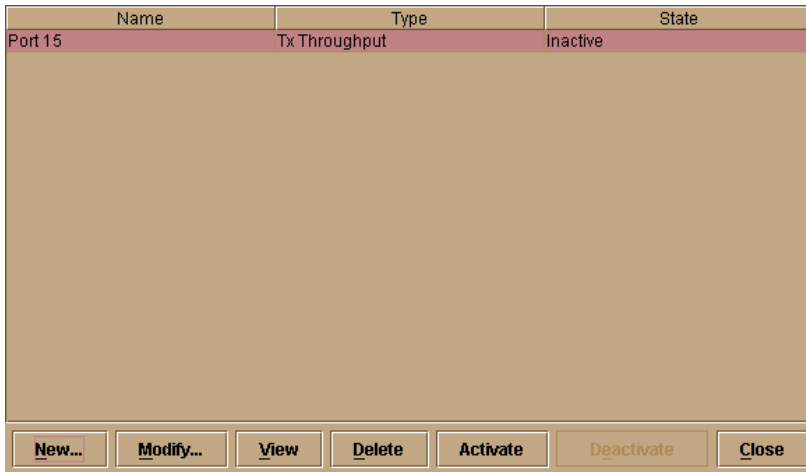
11. Click **Next**. A final screen displays to provide a summary of your alert configuration. To make any changes, backwards and forwards through the configuration screens by selecting **Previous** and **Next**, as shown in Figure 2–33.
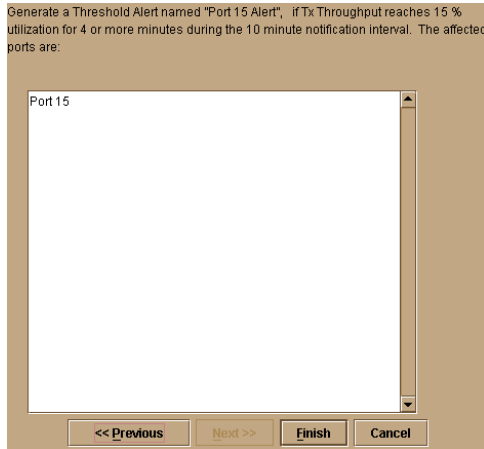
Figure 2–33: New Threshold Alerts dialog box—summary screen

12. Select **Finish**. The **Configure Threshold Alerts** dialog box displays listing the name, type, and state of the alert that you just configured.

At this point, the alert is not active. To activate the alert, select the alert information that displays in the **Configure Threshold Alerts** table and select **Activate**, as shown in Figure 2–34.

Name	Type	State
Port 15	Tx Throughput	Inactive

| New... | Modify... | View | Delete | Activate | Deactivate | Close |

Figure 2–34: Configure Threshold Alerts dialog box—alerts activated

Modify an Alert

Use the following steps to modify an existing threshold alert configuration.

1. Choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays.

2. Select the alert that you want to modify by clicking the alert information in the table.

3. If the alert is active, click **Deactivate**, then select the alert information in the table again.

4. Click **Modify**.

NOTE: If the alert is active, an error message displays prompting you deactivate the alert.

An initial Modify Threshold screen displays where you can change the threshold type.

5. Choose a threshold type from the drop-down list.

6. Click **Next** when you are done. A Modify Threshold screen displays where you can change the **% utilization**, cumulative minutes for the threshold to occur before notification, and the time interval for measuring throughput and for alert notification.

7. Make appropriate changes, then continue through the Modify Threshold screens, making changes as necessary, until the summary screen displays showing the alert configuration.

8. Perform either of the following steps:

   • If you need to change any parameters, select **Previous** and **Next** to display the desired Modify Threshold screen.

   • Select **Finish** when you are done.

Activate or Deactivate Alerts

Use the following steps to activate or deactivate existing threshold alerts. In the active state, notifications are generated for the alert. In the inactive state, notifications do not occur.

1. Choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays. The port's current state, deactive or active, is listed under the **State** column.

2. To change the state, select the alert information in the table.

   • If the alert is active, click **Deactivate** to change to the deactive state.

   • If the alert is deactive, click **Activate** to change to the active state.

Delete Alerts

Use the following steps to delete existing threshold alerts.

1. Choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays.

2. Select the alert that you want to delete by selecting the alert information in the table.

3. Click **Delete**. A message displays asking you to confirm the deletion.

4. Click **Yes**. The alert is removed from the dialog box.

Task 13: Test Remote Notification (Optional)

If the call-home and e-mail notification features are enabled, set up the *HAFM* application to test these remote notification features. Because the features are configured at the *HAFM* application, call-home and e-mail notification are enabled for multiple switches or HP managed products. To test remote notification:

1. Close the **Hardware View** page for the switch and return to the **Product View** page by closing the window.

2. At the **Product View** page, choose **Maintenance** > **Test Remote Notification**. The **Test Remote Notification** dialog box displays, as shown in Figure 2–35.
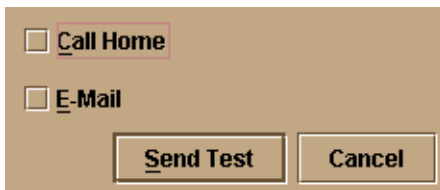
Figure 2–35: Test Remote Notification dialog box

3. Choose **Call Home** and **E-Mail** to perform applicable tests.

   The call home test provides a test notification message to a remote support center. Depending on the option chosen during HAFM installation, the test notification message is transmitted over telephone lines or LAN.

4. Click **Send Test**. Call-home and e-mail test messages are transmitted and an **Information** dialog box displays, as shown in Figure 2–36. Click **OK** to close the dialog box.

5. Verify with recipients that call-home and e-mail notifications were received.

Figure 2–36: Information dialog box

Task 14: Back Up HAFM Configuration Data

It is important to back up the HAFM configuration data. This data is used to restore the HAFM server operating environment in case of hard drive failure.

Refer to the *hp StorageWorks HAFM server installation guide* for instructions on backing up the HAFM configuration data.

Once the HAFM configuration data is backed up, go to "Task 16: Cable Fibre Channel Ports" on page 2–69.

Task 15: Configure the Switch from the Embedded Web Server (Optional)

If an HAFM server is not available, use the Embedded Web Server (EWS) interface to configure the Edge Switch 2/32. Selectively perform the following configuration tasks according to the customer's installation requirements:

- Configure the switch ports.

- Configure the switch identification, date and time, operating parameters, and network addresses.

- Configure SNMP trap message recipients.

- Configure user passwords.

NOTE: This section covers the initial set up of the edge switch 2/32. For additional information regarding setting up zoning, zone sets, and SAN management in general, see the online EWS help.

A PC platform with LAN access and standard web browser running Netscape Navigator 4.6 or higher or Microsoft Internet Explorer 4.0 or higher is required. To open the Embedded Web Server interface:

1. Ensure the browser-capable PC and the Ethernet LAN segment (with the switch attached) are connected.

2. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).

3. At the browser, enter the IP address of the switch as the internet uniform resource locator (URL). Use the default IP address of 10.1.1.10, the factory preset of 10.1.1.10, or the IP address configured while performing "Task 3: Configure Network Information" on page 2–6. The **Username and Password Required** dialog box displays, as shown in Figure 2–37.

Figure 2–37: Username and Password Required dialog box

4.   Type the default user name and password.

NOTE: The default user name is *Administrator* and the default password is *password.* The user name and password are case-sensitive.

---

5.   Click **OK**. The Embedded Web Server interface opens with the **View** window displayed, as shown in Figure 2–38.
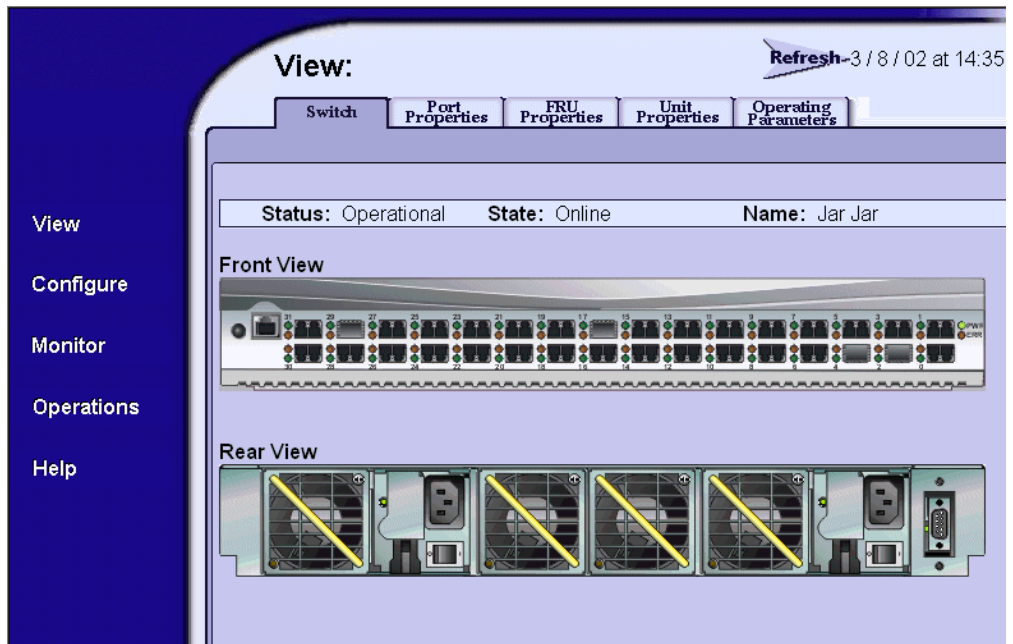
Figure 2–38: Embedded Web Server interface—View window

Configure Switch Ports

Perform the procedure in this section to configure names and operating characteristics for the switch ports.

To configure one or more ports:

1. At the **View** window, click **Configure** at the left side of the window. The **Configure** window opens with the **Ports** tab displayed.

    a. For each port to be configured, type a port name of 24 alphanumeric characters or less in the associated **Name** field. The port name should identify the device to which the port is attached.

    b. Choose the check box in the **Blocked** column to block or unblock a port (default is unblocked). A check mark in the box indicates the port is blocked. Blocking a port prevents the attached device from communicating with the switch. A blocked port continuously transmits the offline sequence (OLS), as shown in Figure 2–39.
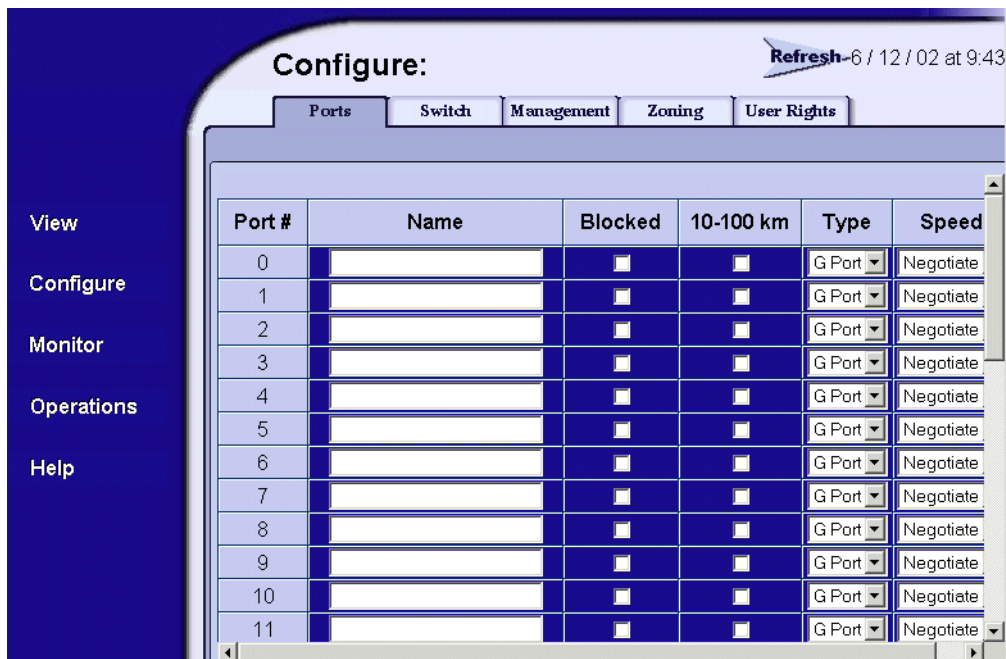

**Figure 2–39: Block or unblock a port from the Configure window**

     c.   Choose the check box in the **10-100 km** column to enable extended distance buffering for a port (default is disabled). A check mark in the box indicates extended distance operation up to 100 kilometers (through repeaters) is enabled.

     d.   Select a **Type** field and choose generic port (**G_Port**), fabric port (**F_Port**), or expansion port (**E_Port**) from the list box. If **F_Port** or **E_Port** is selected, the port will only operate as the port type selected. If **G_Port** is selected, the port type is automatically detected and will operate as an E_Port or F_Port.

     e.   Click the **Speed** field for a port. A **Speed** drop-down list displays. Choose 1 Gb/sec, 2 Gb/sec, or Navigate as the desired setting depending on the speed capability of the device to be plugged into the port.

2.   Click **Activate** to save the information. The message `Your changes to the port configuration have been successfully activated` displays.

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person. The *Name*, *Location*, and *Contact* variables configured here correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. These variables are used by SNMP management workstations when obtaining data from managed switches.

To configure the switch identification:

1.   At the **Configure** window, click the **Switch** tab. The **Switch** page displays with **Identification** tab selected, as shown in Figure 2–40.
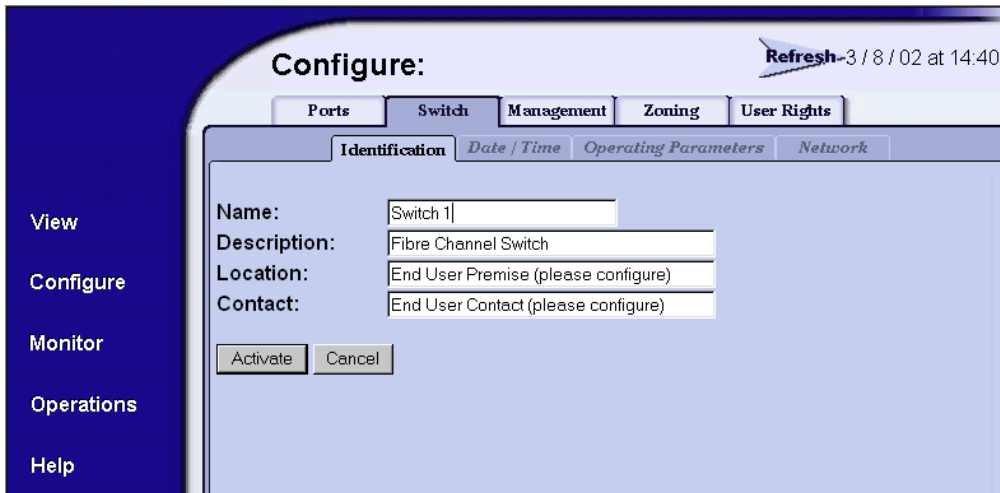
Figure 2–40: Switch page—Identification tab

a. Type a switch name of 24 alphanumeric characters or less in the **Name** field. Each switch should be configured with a unique name.

If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network DNS host name. For example, if the DNS host name is hpes232.hp.com, then enter `hpes232`.

b. Type a switch description of 255 alphanumeric characters or less in the **Description** field.

c. Type the switch physical location (255 alphanumeric characters or less) in the **Location** field.

d. Type the name of a contact person (255 alphanumeric characters or less) in the **Contact** field.

2. Click **Activate** to save the information. The message `Your changes to the identification configuration have been successfully activated` displays.

Configure Date and Time

Perform this procedure to configure the effective date and time for the switch. To set the date and time:

1. At the **Configure** window, click the **Switch** tab, then select **Date/Time** tab. The Switch page displays with **Date/Time** tab selected (highlighted red), as shown in Figure 2–41.
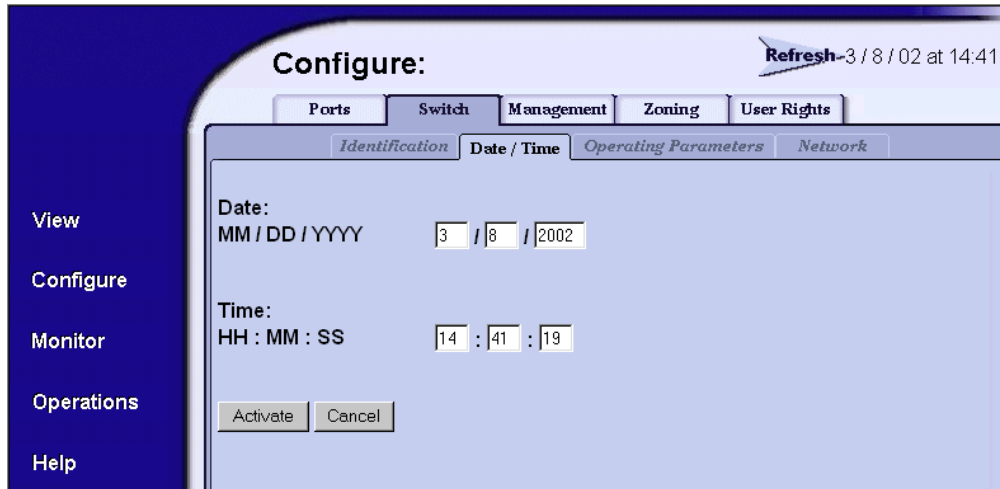
Figure 2–41: Switch page—Date/Time tab

   a. Click the **Date** fields that require change, and type numbers in the following ranges:

   Month (MM): 1 through 12
Day (DD): 1 through 31
Year (YY): greater than 1980

   b. Click the **Time** fields that require change, and type numbers in the following ranges:

   Hour (HH): 0 through 23
Minute (MM): 0 through 59
Second (SS): 0 through 59

2. Click **Activate** to save the information. The message `Your changes to the date/time configuration have been successfully activated` displays.

Configure Switch and Fabric Parameters

Perform this procedure to configure the following switch and fabric operating parameters: Buffer-to-Buffer Credit (BB_Credit), Error Detect Time Out Value (E_D_TOV), and Resource Allocation Time Out Value (R_A_TOV), preferred domain ID and switch priority.

Configure Switch Parameters

The switch must be set offline to configure operating parameters. To configure the parameters:

1. Set the switch offline as follows:

    a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch Beacon** page displayed.

    b. At the **Current State** window, click **Set Offline**. The message Your operations changes have been successfully activated displays.

2. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.

3. At the **Configure** panel, click the **Switch** tab, then select **Parameters**. The **Switch** page displays with **Switch Parameters** displayed.

4. Set the switch parameters:
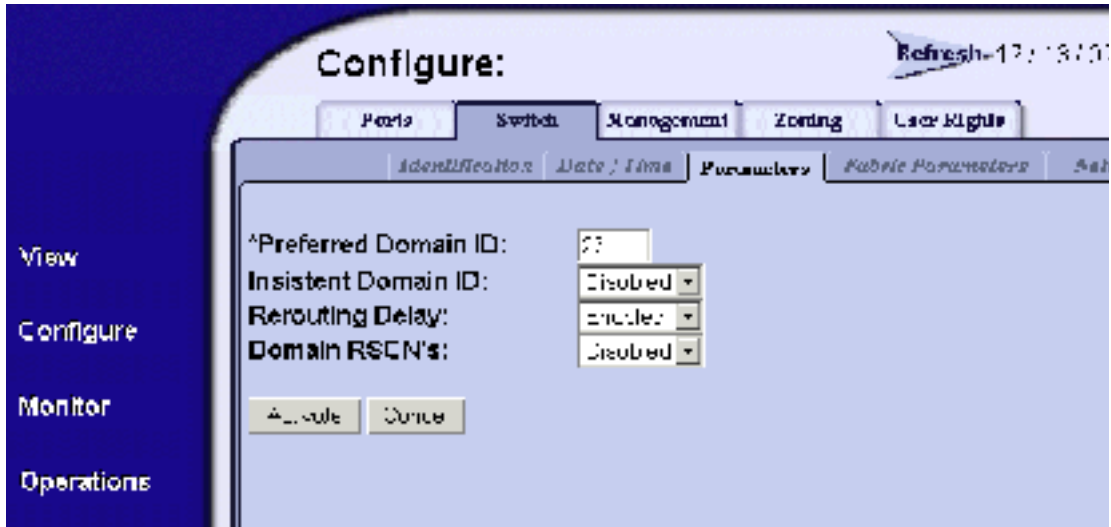
Figure 2–42: Switch page—Parameters tab

a. At the **Preferred Domain ID** field, type a value between 1 and 31 (default is 1). The domain ID uniquely identifies each switch in a fabric.

All fabric-attached switches must have unique domain IDs. If the value is not unique, the E_Port connection to the switch segments and the switch cannot communicate with the fabric.

b. **Insistent Domain:** This option is not supported unless the SANtegrity feature is installed. Click the check box to remove or add a check mark. The default state is disabled (no check mark).

When a check mark displays, the domain ID configured in the **Preferred Domain ID** field will become the active domain identification when the fabric initializes. See the following notes:

— This option is required if High Availability Fabric Manager (HAFM) is enabled.

— If you enable **Insistent Domain** while the switch or director is online, the **Preferred Domain ID** will change to the current active domain ID if the IDs are different.

c. Click the **Rerouting Delay** check box to enable or disable the option. If a check mark displays, the option is enabled. If rerouting delay is enabled, traffic is delayed through a fabric by the specified E_D_TOV time. This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.

d. **Domain RSCNs:** Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. Note that this option is required if High Availability Fabric Manager (HAFM) is enabled.

5. Click **Activate** to save the information. The message Your changes to the operating parameters configuration have been successfully activated displays.

Set Fabric Parameters

The switch must be set offline to configure fabric parameters. To configure the parameters:

1. Set the switch offline as follows:

   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch Beacon** page displayed.

   b. At the **Current State** window, click **Set Offline**. The message Your operations changes have been successfully activated displays.

2. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.

3. At the **Configure** panel, click the **Switch** tab, then select **Fabric Parameters**. The **Switch** page displays with **Fabric Parameters**.

4. Set the fabric parameters:
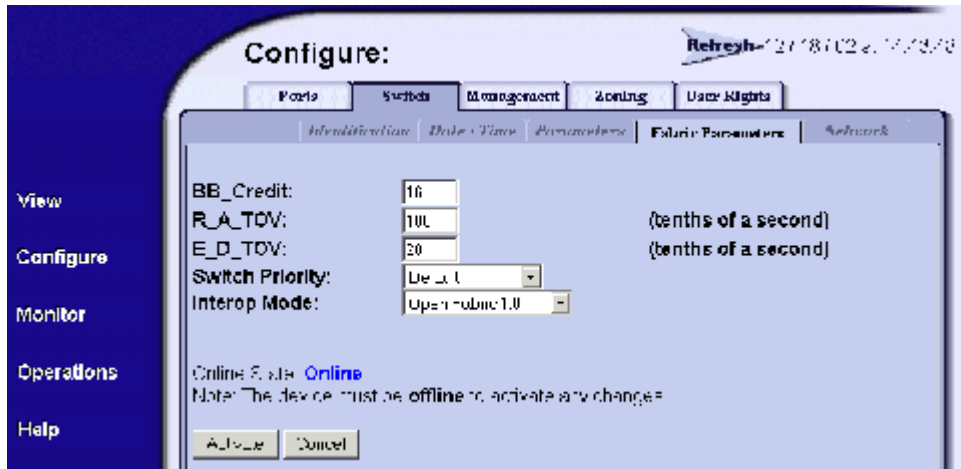
Figure 2–43: Switch page—Fabric Parameters tab

- a. At the **BB_Credit** field, type a value between 1 an 60 buffers. The default is 16. Use a value of 60 buffers only for extended distance port operation.

- b. At the **R_A_TOV field**, type a value between 10 through 1200 tenths of a second (one through 120 seconds). The default is 10 seconds (100 tenths).

  All fabric-attached switches must be set to the same R_A_TOV. If the value is not compatible, the E_Port connection to the switch segments and the switch cannot communicate with the fabric. In addition, the R_A_TOV must be greater than the E_D_TOV.

- c. At the **E_D_TOV** field, type a value between 2 through 600 tenths of a second (0.2 through 60 seconds). The default is 20 tenths of a second (2 seconds).

  All fabric-attached switches must be set to the same E_D_TOV. If the value is not compatible, the E_Port connection to the switch segments and the switch cannot communicate with the fabric. In addition, the E_D_TOV must be less than the R_A_TOV.

- d. The switch priority value designates the fabric's principal switch. The principal switch controls the allocation and distribution of domain IDs for all fabric directors and switches (including itself). At the **Switch Priority** field, select **Principal**, **Never Principal**, or **Default** (the default setting is **Default**).

- e. Select the Interop Mode:

— HP Fabric 1.0. Default. Select this mode if the fabric contains only HP switches and switches that are operating in HP Fabric 1.0 mode.

— Open Fabric 1.0. Select this mode if the fabric contains HP directors and switches, as well as other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

5. Click **Activate** to save the information. The message Your changes to the operating parameters configuration have been successfully activated displays.

6. Set the switch online:

   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch Beacon** page displayed.

   b. At the **Operations** panel, click the **Online State** tab, then click **Set Online**. The message Your operations changes have been successfully activated displays.

Configure Network Information

Verify the type of LAN installation with the customer's network administrator. If one switch is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change. Go to "Configure Ports (Open Systems Mode)" on page 2–32.

If multiple switches are installed, or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme. Perform one of the following:

• If network information was changed while performing "Task 3: Configure Network Information" on page 2–6, this procedure is not required. Go to "Configure SNMP Trap Message Recipients" on page 2–39.

• If network information was not changed, perform this procedure.

Perform the following steps to change a switch IP address, subnet mask, or gateway address.

1. Choose **Configure** at the left side of the window. The **Configure** window opens with the **Ports** page displayed.

2. At the **Configure** window, click the **Switch** tab, then click the **Network** tab. The **Switch** page displays with the **Network** tab selected, as shown in Figure 2–44.
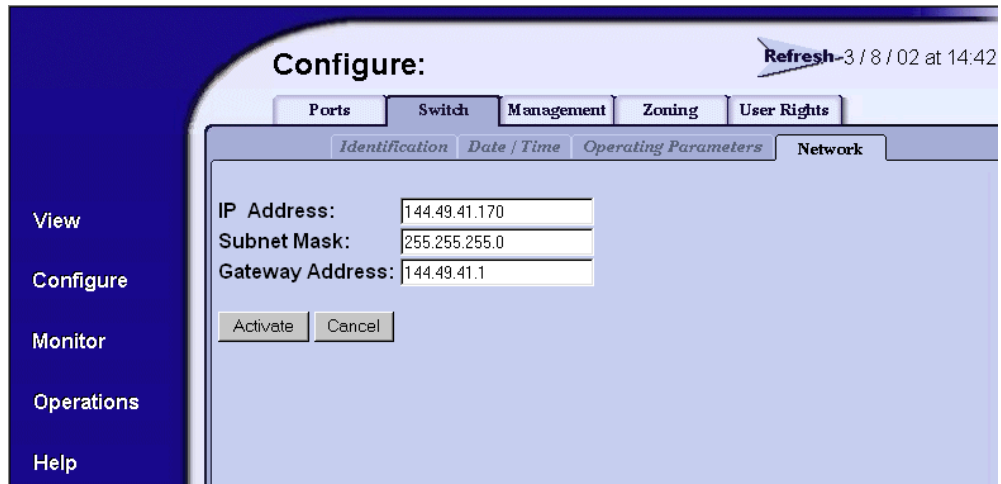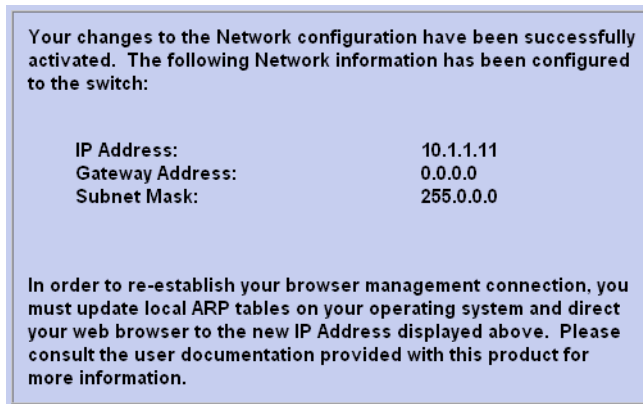
Figure 2–44: Switch page—Network tab

> a. At the **IP Address** field, type the new value as specified by the customer's network administrator (default is *10.1.1.10*, factory preset is *10.1.1.10*).
>
> b. At the **Subnet Mask** field, type the new value as specified by the customer's network administrator (default is *255.0.0.0*).
>
> c. At the **Gateway Address** field, type the new value as specified by the customer's network administrator (default is *0.0.0.0*).

3. Click **Activate** to save the information. The following message box displays, as shown in Figure 2–45.

> Your changes to the Network configuration have been successfully activated. The following Network information has been configured to the switch:
>
> | | |
> | --- | --- |
> | IP Address: | 10.1.1.11 |
> | Gateway Address: | 0.0.0.0 |
> | Subnet Mask: | 255.0.0.0 |
>
> In order to re-establish your browser management connection, you must update local ARP tables on your operating system and direct your web browser to the new IP Address displayed above. Please consult the user documentation provided with this product for more information.

Figure 2–45: Network configuration changes activated

4. Update the address resolution protocol (ARP) table for the browser PC.

   a. Choose **File >Exit** to close the Embedded Web Server and browser applications. The Windows desktop displays.

   b. Choose **Start > Programs** > **Command Prompt**. A disk operating system (DOS) window displays.

   c. Delete the switch's *old* IP address from the ARP table. At the command (C:\) prompt, type arp —d xxx.xxx.xxx.xxx, where xxx.xxx.xxx.xxx is the old IP address for the switch.

   d. Click close (**X**) at the upper right corner of the DOS window to close the window and return to the Windows desktop.

5. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).

6. At the browser, enter the switch's *new* IP address as the Internet URL. The **Username and Password Required** dialog box displays.

7.   Type the default user name and password.

NOTE: The default user name is *Administrator* and the default password is *password.* The user name and password are case-sensitive.

---

8.   Click **OK**. The Embedded Web Server interface opens with the **View** window displayed.

Configure SNMP Trap Message Recipients

Perform this procedure to configure community names, write authorizations, and network addresses and for up to 6 SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs.

To configure SNMP trap recipients:

1.   Choose **Configure** at the left side of the window. The **Configure** window opens with the **Ports** tab displayed.

2.   At the **Configure** window, click the **Management** tab. The **Management** page displays with **SNMP** tab selected, as shown in Figure 2–46.
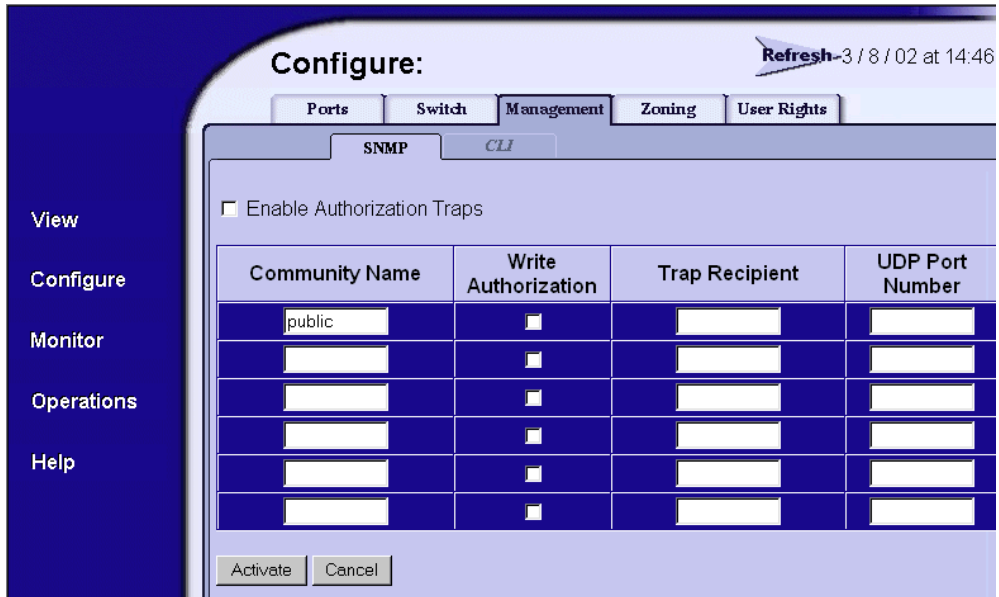
Figure 2–46: Management page—SNMP tab

    a. For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.

    b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.

    c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 64 alphanumeric characters or less. It is recommended the IP address be used.

    d. The default user datagram protocol (UDP) port number for trap recipients is *162*. Type a decimal port number in the associated **UDP Port Number** field to override the default.

3. Click **Activate** to save the information. The message Your changes to the
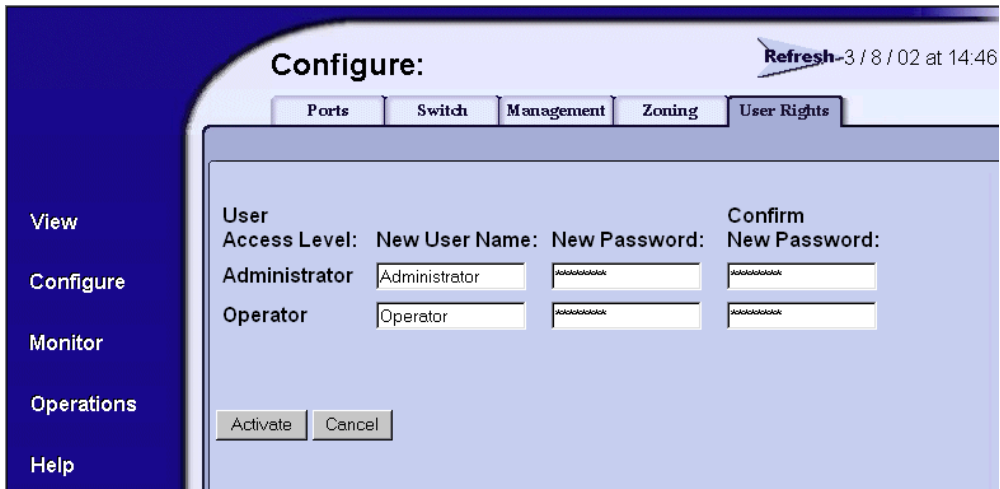   SNMP configuration have been successfully activated
   displays.

Configure User Rights

Perform this procedure to configure the administrator-level and operator-level
passwords used to access the Embedded Web Server interface through the **Username
and Password Required** dialog box.

To configure passwords:

1. At the **Configure** window, click the **User Rights** tab. The **User Rights** page
   displays.

2. For the **Administrator** set of data fields:

   a. Type the administrator user name (as specified by the customer's network
      administrator) in the **New User Name** field. Use 16 alphanumeric characters
      or less.

   b. Type the administrator password (as specified by the customer's network
      administrator) in the **New Password** field. Use 16 alphanumeric characters or
      less.

c.   Type the administrator password again in the **Confirm New Password** field, as shown in Figure 2–47.

Figure 2–47: User Rights page

3.   For the **Operator** set of data fields:

a.   Type the operator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.

b.   Type the operator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.

c.   Type the operator password again in the **Confirm New Password** field.

4.   Click **Activate** to save the information. The message Your changes to the user rights configuration have been successfully activated displays.

5.   Close the browser application by choosing **File > Close**.

Task 16: Cable Fibre Channel Ports

Perform this task to connect devices to the switch. To cable Fibre Channel ports:

1. Route singlemode or multimode fiber-optic cables (depending on the type of SFP pluggable optic transceivers installed) from customer-specified devices to ports at the front of the switch.

2. Connect device cables to small form factor pluggable (SFP) transceivers. Start with port 0 and continue sequentially to the left through port 31.

3. Perform one of the following:

   a. If the switch is installed on a table or desk top, bundle and secure the Fibre Channel cables as directed by the customer.

   b. If the switch is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the switch and other equipment (groups of 16 maximum), and secure them as directed by the customer.

4. Set the switch online.

Task 17: Connect Switch to a Fabric (Optional)

To provide Fibre Channel connectivity between public devices and fabric-attached devices, connect the switch to an expansion port (E_Port) of an HP director or switch. The switch port to switch port connection is called an interswitch link (ISL). To fabric-attach the switch and create an ISL:

1. Ensure the switch is defined to the *HAFM* application (defined while performing "Task 6: Configure the Switch to the HAFM Application" on page 2–13.

2. Ensure the preferred domain ID for the switch is unique and does not conflict with the ID of another switch participating in the fabric. To change the domain ID, see "Task 12: Configure the Edge Switch 2/32 Product Manager Applications" on page 2–23.

3. Ensure the R_A_TOV and E_D_TOV values for the switch are identical to the values for all switches participating in the fabric. To change the values, see "Task 12: Configure the Edge Switch 2/32 Product Manager Applications" on page 2–23.

4. Route a multimode or singlemode fiber-optic cable (depending on the type of SFP transceiver installed) from a customer-specified E_Port of the switch to the switch.

5. Connect the switch-attached fiber-optic cable to the port SFP transceiver.

6. If the switch is managed by an attached HAFM server, go to step 7. If the switch is managed by the Embedded Web Server interface:

   a. Choose **View** at the left side of the window. The **View** window opens with the **Switch** tab selected and displayed.

   b. At the **View** window, click the **Port Properties** tab. The **Port Properties** page displays with **0** selected, and port information listed for port 0.

   c. Choose the port number of the port used to make this ISL connection.

   d. Ensure the **Operational State** field displays **Online** and the **Reason** field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, refer to the *hp StorageWorks edge switch 2/32 service manual* to isolate the problem. If no problems are indicated, installation tasks are complete.

7. At the HAFM server's **Product View** page, double-click the switch icon. The **Hardware View** page for the selected switch displays.

8. Double-click the port connector used to make this ISL connection to open the **Port Properties** dialog box, as shown in Figure 2–48.

Port Number	9
Port Name	
Type	G_Port
Operating Speed	2Gb/sec
Fibre Channel Address	000000
Port WWN	
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	No Light
Reason	
Threshold Alert	

Close

Figure 2–48: Port Properties dialog box

9. Ensure the **Link Incident** field displays **None** and the **Reason** field is blank. If an ISL segmentation or other problem is indicated, refer to the *hp StorageWorks edge switch 2/32 service manual* to isolate the problem. If no problems are indicated, installation tasks are complete.

Task 18: Unpack, Inspect, and Install the Ethernet Hub (Optional)

The HAFM server and one or more switches connect through an Ethernet hub installed on a 10/100 Mbps LAN segment. One hub port is required to connect the HAFM server, and one hub port is required to connect each switch. A combination of up to 48 HP products can be configured and managed by a single HAFM server, therefore multiple hubs may be required to provide sufficient port connections. These hubs must be connected in accordance with the hub manufacturer's specifications. HP recommends using a star or hub-and-spoke topology when connecting multiple hubs. The HAFM server must be connected to the center hub, and there should never be more than two hubs between the HAFM server and any switch. Refer to the hub manufacturer's documentation for more detailed information.

For instructions to unpack and inspect one or more Ethernet hubs, and install the hubs in a desktop or rack-mount configuration, refer to the appropriate Ethernet hub documentation.

3

Flexport Upgrade Instructions

This chapter provides instructions for upgrading the edge switch 2/32 from 16 ports to 24 ports and from 24 ports to 32 ports by installing the Edge Switch 2/32 flexport upgrade kit, see Table 1–1 on page 1–11.

Each port expansion kit includes eight optical transceivers, upgrade instructions, and a entitlement certificate containing transaction code for obtaining a software licence key (feature key) through an HP website. The feature key can be enabled in the switch using one of the following methods:

- Configure menus of the Product Manager

- Configure menus of the Embedded Web Server (EWS) for the specific switch

- Through the command line interface (CLI)

Unpack and Inspect the Optics

Unpack and inspect the optics as follows:

- Inspect the shipping container for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.

- Unpack the shipping container and inspect each item for damage. Ensure all items listed on the enclosed bill of materials are included in the container.

- If any items are damaged or missing, please contact a HP authorized service provider or reseller.

Edge Switch 2/32 Upgrade

This section describes how to upgrade from 16 to 24 ports and from 24 to 32 ports.

NOTE: For more information on installing optical transceivers, refer to the *hp StorageWorks SFP transceiver installation instructions.*

Upgrading to 24 Ports

Ports 0 through 15 should already be populated (see Figure 3–1, ❸).

1. Insert 8 new optical transceivers into ports 16 through 23 (see Figure 3–1, ❷) as follows:

    a. To install a new SFP transceiver, position one of the SFP transceivers so that the key is oriented correctly to the port, and insert the transceiver into the port until it is firmly seated and the latching mechanism clicks.

       NOTE: Transceivers are keyed so that they can only be inserted with the correct orientation. If a transceiver doesn't slide in easily, ensure it is correctly oriented. For instructions that are specific to the transceiver model, refer to the transceiver manufacturer's documentation.

    b. Repeat step a for the remaining ports.

2. If you have no more ports to upgrade, go to "Configure Feature Key in Product Manager, EWS, or CLI." If you want to install more ports, continue with "Upgrading to 32 Ports."

❶ Ports 24 to 31
❷ Ports 16 to 23
❸ Ports 0 to 15
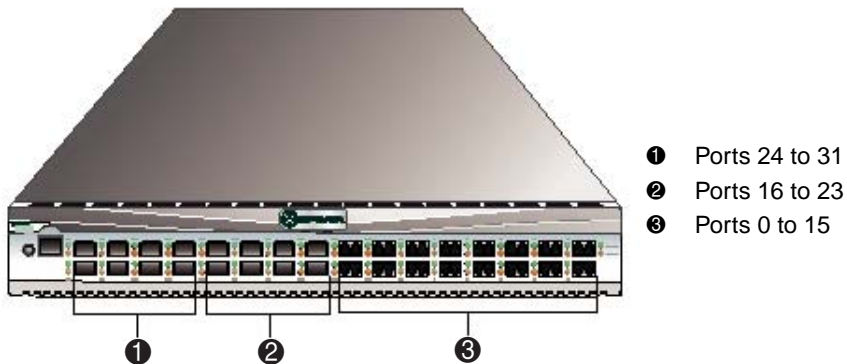
Figure 3–1: Edge Switch 2/32 port locations

Upgrading to 32 Ports

Ports 0 through 23 should already be populated (see Figure 3–1, ❷ and ❸).

1. Insert 8 new optical transceivers into ports 24 through 31 (see Figure 3–1, ❶).

   a. To install a new SFP transceiver, position one of the SFP transceivers so that the key is oriented correctly to the port, and insert the transceiver into the port until it is firmly seated and the latching mechanism clicks.

      NOTE: Transceivers are keyed so that they can only be inserted with the correct orientation. If a transceiver doesn't slide in easily, ensure it is correctly oriented. For instructions that are specific to the transceiver model, refer to the transceiver manufacturer's documentation.

   b. Repeat step a for the remaining ports.

2. Continue with "Configure Feature Key in Product Manager, EWS, or CLI."

Configure Feature Key in Product Manager, EWS, or CLI

Obtain the required feature key by following the instructions on the firmware feature entitlement certificate for HP StorageWorks Fibre Channel switches. The certificate is included in the Flexport upgrade kit. Store the firmware feature entitlement certificate in a safe place.

A feature key is an alphanumeric string consisting of both uppercase and lowercase characters. The following is an example of a feature key format:

   XxXx-XXxX-xxXX-xX

The total number of characters may vary. The key is case sensitive and must be entered exactly, including the dashes.

The following shows how to configure the feature key using HAFM. If you are using EWS to configure the feature key, refer to the online help in the EWS. If you are using CLI to configure the feature key, refer to the *hp StorageWorks CLI reference guide for director 2/64, edge switch 2/16, and edge switch 2/32*.

After you have obtained the feature key, access HAFM for the switch to be configured. Perform the following steps:

1. Set the switch offline by choosing **Set Online State** from the **Maintenance** menu. For help, refer to the *hp StorageWorks edge switch 2/32 product manager user guide*.

2. Choose **Features** from the **Configure** menu on the menu bar. The **Configure Feature Key** dialog box displays, as shown in Figure 3–2.
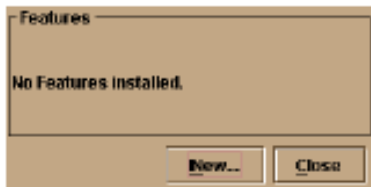
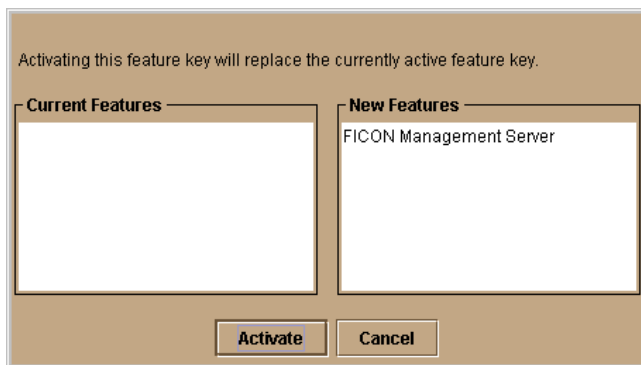

Figure 3–2: Configure Feature Key dialog box

3. Click **New** to add a new feature key. The **New Feature Key** dialog box displays, as shown in Figure 3–3.

Figure 3–3: New Feature Key dialog box

4. In the **New Feature Key** dialog box, enter the switch's feature key and click **OK**. The **Enable Feature Key** dialog box displays, as shown in Figure 3–4.

Figure 3–4: Enable Feature Key dialog box

The **Enable Feature Key** dialog box displays with a warning, stating that this action will override the current set of features on the switch. If features are enabled on the switch, they will be listed in the left column.The list on the right is a set of features that come with the new feature key. All of the features that are currently active on the switch are included in the new feature list.

5. Click **Activate** to activate the new feature key.

   An IPL will occur, during which the Ethernet connection between the HAFM server and switch is momentarily interrupted.

6. Set the switch back online by choosing **Set Online State** from the **Maintenance** menu.

7. When you are finished configuring the switch, you can back up the configuration data. For more information, refer to the *hp StorageWorks edge switch 2/32 product manager user guide*.

NOTE: Be sure to keep the feature entitlement certificate in a secure place.

> **CAUTION:** Performing a configuration reset with HAFM or EWS will reset all configuration data and non-volatile settings to factory default values. This includes features keys. Following a configuration reset, feature keys must be reconfigured.

A

Regulatory Compliance Notices

This appendix covers the following topics:

Regulatory Compliance ID Numbers

For the purpose of regulatory compliance certifications and identification, your HP StorageWorks Director 2/140 is assigned a HP Regulatory Model Number. The HP Regulatory Model Number for this product is:

RSVLB-0214

The HP StorageWorks Director 2/140 Regulatory Model Number can be found on the product label, along with the required approval markings and information. When requesting certification information for this product, always refer to this Regulatory Model Number. This Regulatory Model Number should not be confused with the marketing name or product number for your HP StorageWorks Director 2/140.

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or ID on the label. After the class of the device is determined, refer to the corresponding statement in the sections below.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio or television technician for help.

Declaration of Conformity for Products Marked with FCC Logo—United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, refer to http://thenew.hp.com.

For questions regarding this FCC declaration, contact:

Hewlett-Packard Company
Product Regulations Manager
3000 Hanover St.
Palo Alto, CA 94304

Or call 1-650-857-1501

To identify this product, refer to the part, Regulatory Model Number, or product number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Network and Serial Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

IEC EMC Statement (Worldwide)

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Spécification ATI Classe A (France)

DECLARATION D'INSTALLATION ET DE MISE EN EXPLOITATION d'un matériel de traitement de l'information (ATI), classé A en fonction des niveaux de perturbations radioélectriques émis, définis dans la norme européenne EN 55022 concernant la Compatibilité Electromagnétique.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parenthesis):

• EN55022 1998 (CISPR 22)-Electromagnetic Interference

- EN55024 1998 (IEC61000-4-2, IEC61000-4-3, IEC61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8, IEC61000-4-11)-Electromagnetic Immunity

- EN60950 (IEC60950)-Product Safety

- Power Quality: (IEC610000-3-2)-Harmonics and (IEC61000-3-3)-Voltage Fluctuations and Flicker

- Also approved under UL 1950, 3rd Edition/CSA C22.2 No. 950-95, Safety of Information Technology Equipment

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Notice

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Harmonics Conformance (Japan)

高調波ガイドライン適合品

German Noise Declaration

Schalldruckpegel Lp = 66.8 dB(A)
Am Arbeitsplatz (operator position)
Normaler Betrieb (normal operation)
Nach ISO 7779:1988 / EN 27779:1991 (Typprüfung)

Laser Safety

⚠ **WARNING: To reduce the risk of exposure to hazardous radiation:**
- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the laser device.

Laser Safety (Finland)

LASERTURVALLISUUS

LUOKAN 1 LASERLAITE

KLASS 1 LASER APPARAT

Fibre Channel -kytkinlaitteessa on 16 optista liitäntäporttia, joissa on laserdiodin sisältävä lähetinosa. Fibre

Channel -kytkinlaite on käyttäjälle turvallinen luokan 1 laserlaite, eikä käyttäjä voi altistua turvallisuusluokan 1 ylittävälle lasersäteilylle toimiessaan käyttöohjeen mukaisesti.

Laitteen turvallisuusluokka on määritetty standardin EN 60825-1 (1994) mukaisesti.

VAROITUS !

Laitteen käyttäminen muulla kuin käyttöohjeessa mainitulla tavalla saattaa altistaa käyttäjän turvallisuusluokan 1 ylittävälle näkymättömälle lasersäteilylle.

VARNING !

Om apparaten används på annat sätt än i bruksanvisning specificerats, kan användaren utsättas för osynlig laserstrålning, som överskrider gränsen för laserklass 1.

Fibre Channel -kytkinlaitteessa ei ole käyttäjän tehtäväksi tarkoitettuja huolto- tai säätötoimenpiteitä. Laitteen saa avata ja huoltaa ainoastaan sen huoltamiseen koulutettu henkilö.

Tiedot laitteessa käytettävän laserdiodin säteilyominaisuuksista:

Aallonpituus 850 nm

Certification and Classification Information

This product contains a laser internal to the Optical Link Module (OLM) for connection to the Fibre communications port.

In the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. The certification is indicated by a label on the plastic OLM housing.

Outside the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in IEC 825-1:1993 and EN 60825-1:1994, including Amendment 11:1996.

The OLM includes the following certifications:

- UL Recognized Component (USA)
- CSA Certified Component (Canada)
- TUV Certified Component (European Union)
- CB Certificate (Worldwide)

The following figure shows the Class 1 information label that appears on the metal cover of the OLM housing.

CLASS 1
LASER PRODUCT

LASER KLASSE 1
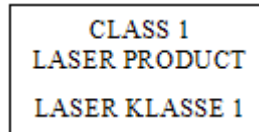
Declaration of Conformity

The Declaration of Conformity is shown on the next page.

B

Technical Specifications

This appendix contains the following information:

- Factory Defaults, page B–1

- Physical Dimensions, page B–3

- Environmental Specifications, page B–4

- Power Requirements, page B–4

- Operating Tolerances, page B–4

- Laser Information, page B–5

Factory Defaults

Table B–1 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table B–1: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Table B–2 gives the Switch factory-default values for Reset Configuration option.

**Table B–2: Switch Factory-Default Values for Reset
Configuration Option**

Configuration	Description	Default
Identification	Switch Name	NULL string
	Switch Description	"Fibre Channel Switch"
	Switch Contact	"End User Contact (please configure)"
	Switch Location	"End User Contact (please configure)"
Ports	Port Names	NULL strings
	Port Blocked States	Unblocked
	Extended Distance (10-100km)	Disabled
	LIN Alerts	Disabled
	Port Address	Port number plus 4
	Ports enabled	16
Switch Addressing	IP Address	10.1.1.10
	Subnet Mask	255.0.0.0
	Gateway Address	0.0.0.0
	MAC Address	PROM value
Operating Mode	Must select one of two modes: Homogeneous mode or Open Fabric 1.0. The recommended mode is Open Fabric 1.0.	Homogeneous mode
Operating Parameters	Preferred Domain ID	1
	Buffer-to-Buffer Credit	60
	R_A_TOV	10 seconds (100 tenths)
	E_D_TOV	2 seconds (20 tenths)
	Switch Priority	Default
	Switch Speed	2 Gb/sec
	Rerouting Delay	Disabled

Table B–2: Switch Factory-Default Values for Reset Configuration Option (Continued)

Configuration	Description	Default
SNMP	SNMP Communities	"public" — 5 NULL strings
	SNMP Write Authorizations	Read only per community
	Trap Recipient IP Addressees	0 for each
	UDP Port	162
	SNMP Authorization Trap State	5
Management Server	Active Equal Saved State	Disabled
	Remote Offline Control State	Disabled
Zoning	Number of Zone Members	0
	Number of Zones	0
	Number of Zone Sets	0
	Zone Names	None
	Zone Sets Names	None
	Zone Members	None
	Default Zone State	Enabled
	Active Zone Set State	Disabled
	Active Zone Set Name	NULL string

Physical Dimensions

Table B–3 lists edge switch 2/32 dimensions.

Table B–3: Dimensions

Dimension	Size
Height	6.47 cm (2.55 in)
Width	44.5 cm (17.5 in)
Depth	66.8 cm (26.7 in)
Weight	15.4 kg (34 lb)
Shipping Weight	17.2 kg (38 lb)

Environmental Specifications

Figure B–4 lists environmental ranges for shipping, storing, and operating the hp StorageWorks edge switch 2/32.

Table B–4: Environmental Specifications

Specification	Shipping	Storage	Operating
Weight	17.2 kg (38 lb)	15.4 kg (34 lb)	15.4 kg (34 lb)
Temperature	-40° F to 140° F (-40° C to 60° C)	34° F to 140° F (1° C to 60° C)	40°F to 104°F (4°C to 40 °C)
Humidity	5% to 100%	5% to 80%	8% to 80%
Maximum wet-bulb temperature	84° F (29° C)	84°F (29°C)	81°F (27°C)
Altitude	40,000 ft (12,192 m)	40,000 ft (12,192 m)	10,000 ft (3,048 m)

Power Requirements

Table B–5 lists edge switch 2/32 power requirements.

Table B–5: Power Requirements

Specification	Value
Input voltage	100 to 240 VAC
Input frequency	47 to 63 Hz

Operating Tolerances

Table B–6 lists heating and cooling specifications, shock tolerances, vibration, acoustical noise and inclination.

Table B–6: Operating Tolerances

Specification	Value
Heat dissipation	836 BTU/hr (32 ports)
Cooling airflow clearances	Right and left sides: No clearance required Front and rear: 7.6 cm (3.0 in) Top and bottom: No clearance required

Table B–6: Operating Tolerances (Continued)

Specification	Value
Shock and vibration tolerance	60 Gs for 10 milliseconds without nonrecoverable errors
Acoustical noise	6.6 Bels
Inclination	10° maximum

Laser Information

Three configurations of cards with fixed optics will be provided for each of the connector types: four extended long-wave ports, four long-wave ports, and four short-wave ports.

Table B–7: Laser specs — 2 Gb

Part Number	Transceivers on UPM Card	Wave Length	Media/Distance	Standard
300836-B21 Long wave — 35 Km	4 Extended Long wave	1310 nm	*9/125* µm Single-mode: 1 m–35 Km	100-SM-LL-L
300835-B21 Long wave — 10 Km	4 Long wave	1310 nm	*9/125* µm Single-mode: 1 m–10 Km	100-SM-LL-L
300834-B21 Short wave	4 Short wave	850 nm	*50/125* µm Multimode: 2 m–500 m *62.5/125* µm Multimode: 1 m–200 m	100-M5-SN-I

Glossary

This glossary defines terms used in this guide or in other guides in this series, and is not a comprehensive glossary of computer terms.

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposite or substantively different meaning.

See. This refers the reader to another keyword or phrase for the same term.

See also. This refers the reader to additional information contained in another entry.

access control
List of all devices that can access other devices across the network and the permissions associated with that access. *See also* persistent binding and zoning.

active FRU
A field-replaceable unit that is currently operating as the active and not the backup FRU.

active zone set
Single zone set that is active in a multi-switch fabric. It is created when you enable a specified zone set. This zone set is compiled by checking for undefined zones or aliases.

agent
Software that processes queries on behalf of an application and returns replies.

alarm
SNMP message notifying an operator of a network or device problem.

alias server
Fabric software facility that supports multicast group management.

arbitration
Process of selecting one device from a collection of devices that request service simultaneously.

audit log
Log summarizing actions (audit trail) made by the user.

authentication
Verification of identity for a person or process.

backplane
The backplane provides 48 VDC power distribution and connections for all logic cards.

backup FRU
When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain director and Fibre Channel link operation.

beaconing
Use of light-emitting diodes on ports, port cards, field-replaceable units, and directors to aid in the fault-isolation process; when enabled, active beaconing will cause LEDs to flash for selected components.

BB_Credit
Also known as Buffer-to-Buffer Credit. Indicates the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device.

ber
See bit error rate.

bidirectional
In Fibre Channel, the capability to simultaneously communicate at maximum speeds (100 Mbps) in both directions over a link.

bit error rate
Ratio of received bits that contain errors to total of all bits transmitted.

blocked port
Devices communicating with the port are prevented from logging into the director or communicating with other devices attached to the director. A blocked port continuously transmits the offline sequence.

bridge
Device that connects and passes packets between two network segments that use the same communications protocol.

broadcast
Send a transmission to all N_Ports on a fabric.

broadcast frames
Data packet, also known as a broadcast packet, whose destination address specifies all computers on a network. *See also* multicast.

buffer
Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See* also BB_Credit.

CHPID
See channel path identifier.

call-home
Product feature which enables the HAFM server to automatically contact a support center and report system problems. The support center server accepts calls from the HAFM server, logs reported events, and can notify one or more support center representatives.

channel
Point-to-point link that transports data from one point to the other.

channel path
A single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests.

channel path identifier
In a channel subsystem, a value assigned to each installed channel path of the system that uniquely identifies that path to the system.

channel wrap test
A diagnostic procedure that checks host-to-Director connectivity by returning the output of the host as input. The test is host-initiated, and transmits Fibre Channel frames to a director port. A director port enabled for channel wrapping echoes the frame back to the host.

class of Fibre Channel service
Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

Class F Fibre Channel service
Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multi-switch fabric.

Class 2 Fibre Channel service
Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two N_Ports. In-order delivery of frames is not guaranteed.

Class 3 Fibre Channel service
Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two N_Ports. Also known as datagram.

community profile
Information that specifies which management objects are available to what management domain or SNMP community name.

concurrent maintenance
Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units, while a hardware product is operating.

configuration data
Configuration data includes: identification data, port configuration data, operating parameters, SNMP configuration, and zoning configuration. A configuration backup file is required to restore configuration data if the CTP2 card in a non-redundant director is removed and replaced.

connectionless
Non-dedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this to the dedicated bandwidth that is required in a Class 1 Fibre Channel Service point-to-point link.

connector
See optical fiber connector.

control processor card
Circuit card that contains the director microprocessor. The CTP2 card also initializes hardware components of the system after power-on. A 10 Mbps RJ-45 twisted pair connector is located on the CTP2 card to connect to the Ethernet LAN and communicate with the HAFM server or a specific management station.

control unit
A hardware unit that controls the reading, writing, or displaying of data at one or more input/output units.

control unit port
An internal director port on the CTP2 card that communicates with the attached processor channels to report error conditions and link initialization.

CRC
See cyclic redundancy check.

CTP2
See control processor card.

CUP
See control unit port.

cyclic redundancy check
System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

DASD
Direct access storage device such as a disk drive.

datagram
See Class 3 Fibre Channel service.

default
Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.

default zone
Contains all attached devices that are not members of a separate zone.

destination address
Address identifier that indicates the targeted destination of a data frame.

device
Product, connected to a managed director, that is not controlled directly by the Product Manager. *See also* node.

diagnostics
Procedures used by computer users and service personnel to diagnose hardware or software error conditions.

dialog box
Dialog box is a window containing informational messages or data fields to be modified or filled in with desired options.

D_ID
See destination address.

Director
An intelligent Fibre Channel switching device providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

DNS name
Domain name system or domain name service. Host or node name for a device or managed product that is translated to an IP address through a domain name server.

domain ID
Number (1 through 31) that uniquely identifies a switch in a multi-switch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch.

E_Port
See expansion port.

port card map
Map showing numbers assigned to each port card by card slot.

Product Manager
Application that implements the management user interface for the director.

E_D_TOV
See error-detect time-out value.

Embedded Web Server
Administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the director through an Embedded Web Server interface. The interface provides a GUI similar to the *Product Manager* application, and supports director configuration, statistics monitoring, and basic operation.

error detect time out value
E_D_TOV defines the time the switch waits for an expected response before declaring an error condition.

error message
Indication that an error has been detected. *See also* information message and warning message.

Ethernet
A widely implemented local area network (LAN) protocol that uses a bus or star topology and served as the basis for the IEEE 802.3 standard, which specifies the physical and software layers. Baseband LAN allows multiple station access to the transmission medium at will without prior coordination and which avoids or resolves contention.

Ethernet hub
A device used to connect the HAFM server and the directors it manages.

event code
Code that provides the operator with information concerning events.

event log
Record of significant events that have occurred on the director, such as FRU failures, degraded operation, and port problems.

expansion port
Physical interface on a Fibre Channel switch within a fabric, that attaches to an expansion port (E_Port) on another Fibre Channel switch to form a multi-switch fabric. *See also* segmented E_Port.

explicit fabric login
Data field size, supported by an F_Port, that is agreed upon during fabric login.

fabric
Entity that interconnects N_Ports and is capable of routing (switching) Fibre Channel frames using the destination ID information in the Fibre Channel frame header accompanying the frames.

fabric element
Any active director or node in a switched fabric.

fabric port
Physical interface within the fabric that connects to an N_Port through a point-to-point full duplex connection.

failover
Automatic and non-disruptive transition of functions from an active FRU that has failed to a backup FRU.

FCC-IOC
See Fibre Channel I/O controller.

FE-MIB
See Fibre Channel fabric element.

fiber
Physical media types supported by the Fibre Channel specification, such as optical fiber, twisted pair, and coaxial cable.

fiber optics
Branch of optical technology concerned with the transmission of light pulses through fibers made of transparent materials such as glass, fused silica, and plastic.

fiber port module card
Each fiber port module card provides four Fibre Channel connections through duplex small form factor (SFF) pluggable fiber-optic transceivers.

Fibre Channel
Integrated set of standards recognized by ANSI which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel fabric element
Any device linked to a fabric. Information about these devices is recorded in a management information base (MIB) which can be accessed by fabric management software.

Fibre Channel I/O controller
A device that controls the embedded Fibre Channel port and configures the ports' ASICs.

field-replaceable unit
Assembly removed and replaced in its entirety when any one of its components fails.

firmware
Embedded program code that resides and executes on the director.

FPM
See fiber port module card.

F_Port
See fabric port.

FRU
See field-replaceable unit.

gateway
A multi-homed host used to route network traffic from one network to another, and to pass network traffic from one protocol to another.

gateway address
A unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a gateway on the network.

generic port
Also known as G_Port. Physical interface on a director that can function either as a fabric port (F_Port) or an extension port (E_Port) depending on the port type to which it connects.

G_Port
See generic port.

hardware log
Record of FRU insertions and removals in the director.

hardware management console
The console runs the *Hardware Management Console* application (HWMCA), and is the operations and management PC platform for 2/Series servers.

HAFM
See also high availability fabric manager.

HBA
See host bus adapter.

high availability
A performance feature characterized by hardware component redundancy (enabling non-disruptive maintenance). High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

High Availability Fabric Manager
A Java-based graphical user interface (GUI) that enables the user to manage users and products, monitor products, and open Product Managers. *See also* HAFM.

hop
Data transfer from one node to another node.

homogeneous fabric
A fabric consisting of only HP products.

hop count
The number of hops a unit of information traverses in a fabric.

host bus adapter
Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

hot-swapping
Removing and replacing a device's components while the device continues to operate normally.

hub
In Fibre Channel, a device that connects nodes into a logical loop by using a physical star topology.

IML
See initial machine load.

inband management
Management of the director through a Fibre Channel connection to a port card.

information message
Message telling a user that a function is performing normally or has completed normally. *See also* error message and warning message.

initial machine load
Also known as IML. Hardware reset for all installed CTP2 cards on the director. It does not affect other hardware. It is initiated by pushing the white button on a director's CTP2 card.

initial program load
Process of initializing the device and causing the operating system to start. Initiated through a menu in the Product Manager, this option performs a hardware reset on the active CTP2 only.

interface
Hardware, software, or both, linking systems, programs, or devices.

internet protocol address
Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability
Ability to communicate, execute programs or transfer data between various functional units over a network.

interswitch link
Also known as ISL. Physical E_Port connection between two directors in a fabric.

I/O configuration
See input/output configuration.

IOCDS
A data set that contains an I/O configuration definition built by the IOCP.

IOCP
See input/output configuration program.

IP address
See internet protocol address.

IPL
See initial program load.

ISL
See interswitch link.

jumper cable
Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable.

latency
When used in reference to a Fibre Channel switching device, latency refers to the amount of time elapsed between receipt of a data transmission at a switch's incoming F_Port (from the originating node port) to retransmission of that data at the switch's outgoing F_Port (to the destination N_Port). The amount of time it takes for data transmission to pass through a switching device.

LIN
See link incident.

link
Physical connection between two devices on a switched fabric.

link incident
Interruption to link due to loss of light or other causes.

load balancing
Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on a director occurs automatically.

logical unit number

Also known as LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's world wide name, represents a unique identifier for a logical device on a storage area network.

loopback plug

In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input.

loopback test

Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LUN

See logical unit number.

MAC address

See media access control address.

maintenance port

Connector on the director where a PC running an ASCII terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product

Hardware product that can be managed with the HAFM. For example, the edge 2/32 is a managed product. *See also* device.

management information base

Related set of software objects (variables) containing information about a managed device and accessed via SNMP from a network management station.

management session

Management session exists when a user logs onto the HAFM server. HAFM can support multiple concurrent management sessions. The user must specify the network address of the server at logon time.

Media Access Control address

Hardware address of a node (device) connected to a network.

MIB

See management information base.

multicast

Delivery of a single transmission to multiple destination N_Ports. Can be one to many or many to many. All members of the group are identified by one IP address.

multi-switch fabric
Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

name server
Program that translates names from one form into another. Domain name servers (DNS) translate domain names into IP addresses.

name server zoning
N_Port access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

network address
Name or address that identifies a managed product on a TCP/IP network. The network address can be either an IP address in dotted-decimal notation containing four three-digit octets in the format xxx.xxx.xxx.xxx), or a domain name (as administered on a customer network).

nickname
Alternate name assigned to a world wide name for a node or director in the fabric.

node
In Fibre Channel terminology, node refers to an end device (server or storage device) that is or can be connected to a switched fabric.

node port
Physical interface within an end device which can connect to an F_Port on a switched fabric or directly to another N_Port (in point-to-point communications).

non-disruptive maintenance
Ability to service FRUs (including maintenance, installation, removal and replacement) while normal operations continue without interruption. *See also* concurrent maintenance.

N_Port
See node port.

offline sequence
Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so.

OLS
See offline sequence.

operating state (Director)
The operating states are described as follows:

> **Online**—when the director is set online, an attached device can log in to the director if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.

Offline—when the director is set offline, all ports are set offline. The director transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the director.

operating state (port)
Valid states include Online, Offline, Testing, Beaconing, Invalid Attachment, Link Incident, No Light, Not Operational, Port Failure, Segmented E_Port.

operating status (Director)
The operating status depends on hardware component failures, which are indicated by alert symbols that display in HAFM application views.

Open Systems Management server
An optional feature that can be enabled on the director or switch through the *Product Manager* application. When enabled, host control and management of the director or switch are provided through an open systems interconnection (OSI) device attached to a director or switch port.

optical cable
Fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications. *See also* jumper cable, optical cable assembly, and trunk cable.

optical cable assembly
Optical cable that is connector-terminated. *See also* jumper cable and optical cable.

optical fiber connector
Hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

out-of-band management
Transmission of management information using frequencies or channels other than those routinely used for information transfer.

packet
Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check).

password
Unique string of characters known to the computer system and to a user who must specify it to gain full or limited access to a system and to the information stored within it.

path
In a network, any route between any two ports.

persistent binding
A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device) using a unit number.

port
Receptacle on a device to which a cable leading to another device can be attached.

port card
Field-replaceable hardware component that provides the port connections for fiber cables and performs specific device-dependent logic functions.

port name
Name that the user assigns to a particular port through the Product Manager.

POST
See power-on self test.

power-on self-test
Series of self-tests executed each time the unit is booted or reset.

preferred domain ID
Domain ID that a switch is assigned by the principal switch in a switched fabric. The preferred domain ID becomes the active domain ID except when configured otherwise by the user.

preventive service planning bucket
Collected problems after early ship of an IBM product.

principal switch
The switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

product name
User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. For the director, the product name can also be accessed by an SNMP manager as the system name.

PSP bucket
See preventive service planning bucket.

R_A_TOV
See resource allocation time-out value.

redundancy
Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hr./7 days per week) computer systems and networks.

remote access link
Connection to a device or program on a computer network via a (geographically) remote workstation.

remote notification
A process by which a system is able to inform remote users and/or workstations of certain classes of events that occur on the system. E-mail notification and the configuration of SNMP trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

remote user workstation
Workstation, such as a PC, running HAFM Software that can access the HAFM server over a LAN connection.

resource allocation time-out value
R_A_TOV is a value used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

SAN
See storage area network.

SBAR
See serial crossbar assembly.

SC
Subscriber connectors.

segmented E_Port
E_Port that has ceased to function as an E_Port within a multi-switch fabric due to an incompatibility between the fabrics that it joins. *See also* expansion port.

SEL
System error light.

serial crossbar assembly
The serial crossbar assembly (SBAR) is responsible for Fibre Channel frame transmission from any director port to any other director port. Connections are established without software intervention.

SNMP
Simple network management protocol. Specifies a mechanism for network management that is complete, yet simple. Information is exchanged between agents, which are the devices on the network being managed, and managers, which are the devices on the network through which the management is done.

SNMP community

Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

SNMP community name

The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

SSP

See system services processor.

storage area network

A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

subnet mask

Used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address.

switchover

Changing a backup FRU to the Active state, and the active FRU to the Backup state.

switch priority

Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch.

system services processor

Controls the RS-232 maintenance port, the Ethernet port, and the operator panel of a Fibre Channel director.

topology

Logical and/or physical arrangement of stations on a network.

trap

Unsolicited notification of an event originating from a SNMP managed device and directed to an SNMP network management station.

trap host

SNMP management workstation that is configured to receive traps.

trunk cable

Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels. *Contrast with* jumper cable.

unblocked port
Devices attached to an unblocked port can login to the director and communicate with devices attached to any other unblocked port assuming that this is supported by the current zoning configuration.

unicast
Communication between a single sender and a single receiver over a network. Compare to *multicast* and *anycast* (communication between any sender and the nearest of a group of receivers).

universal port module card
Each universal port module (UPM) card provides four Fibre Channel connections through duplex small form factor (SFF) pluggable fiber-optic transceivers. UPM cards allow 1 Gb/s and 2 Gb/s operation.

vital product data
System-level data stored by the backplane in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

UPM card
See universal port module card.

VPD
See vital product data.

warning message
Indication that a possible error has been detected. *See als*o error message and information message.

wrap plug
See loopback plu*g*.

World Wide Name
Eight byte address that uniquely identifies a switch, or a node (end device), even on global networks.

WWN
See World Wide Name.

zone
Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot.

zone member
Specification of a device to be included in a zone. A zone member can be identified by the port number of the director to which it is attached or by its world wide name. In multi-switch fabrics, identification of end-devices/nodes by world wide name is preferable.

zone set
See zone.

zoning
Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director, may be configured into one or more zones. *See also* zone.

Index